eric campos bastos guedes

Fórmulas para $\mathbb{N}$úmeros $\mathbb{P}$rimos

Eric Campos Bastos Guedes

Fórmulas para
Números Primos

Ficha catalográfica

G 924 Guedes, Eric Campos Bastos

Fórmulas para números primos: / Eric Campos Bastos Guedes. – Rio de Janeiro: Sociedade Brasileira de Matemática, 2008.

89p.

ISBN: ____________________

1. Números primos. 2 Teoria dos números. 3 Matemática-fórmulas. I. Título

CDD: 512.72

Em memória de meu pai

Agradeço ao professor Jorge Petrúcio Viana
pelo apoio e incentivo.

Prefácio

Uma fórmula para primos é uma função cuja imagem é um conjunto de números primos. Certa vez, mostrei a um grupo heterogêneo de estudantes e professores de Matemática um exemplo de função que produzia todos os primos, e somente primos. A primeira reação foi o espanto de quem sempre ouviu falar que não existiam tais fórmulas. Em seguida, os mais experientes esclareceram que existem infinitas fórmulas para primos. Havendo infinitas, quais serão especialmente elegantes? Breves? Engenhosas? Quais suscitarão questões de interesse? Que conjecturas surgirão de modo natural? Como caracterizar os números primos de modo não trivial? Como construir uma fórmula para primos usando essa caracterização? Essas questões vão sendo respondidas ao longo deste livro, através de exemplos acompanhados de demonstrações. O bom leitor terá a oportunidade de responder a questões que o desenvolvimento das idéias do texto proporciona.

Niterói, maio de 2006.

Eric Campos Bastos Guedes

Sumário

1

Os Números Primos e seus Desafios

Divisibilidade

Seria difícil falar em números primos sem mencionar o conceito de divisibilidade. Se a e b são inteiros quaisquer, então dizemos que b é *divisível* por a sempre que existir um número inteiro q satisfazendo $b=aq$. Dizer que b é divisível por a é o mesmo que dizer: "b é *múltiplo* de a", "a é *divisor* de b", "*a divide b*", ou, em símbolos $a|b$. Escreve-se $a|b$ para significar que b deixa resto zero na divisão por a, isto é, a divisão de b por a é exata. Quando não o for escreveremos $a \nmid b$ (lê-se "a não divide b"). Exemplos: $2|6$, $6|60$, $5 \nmid 6$.

Estando claro o conceito de divisibilidade, podemos falar no conjunto de divisores positivos de um inteiro. Por exemplo, os divisores positivos de 12 são 1, 2, 3, 4, 6 e 12; os de 8 são 1, 2, 4 e 8. Os divisores *comuns* a 12 e 8 são 1, 2 e 4. O maior deles é o 4, e por isto é chamado de *m*áximo *d*ivisor *c*omum de 8 e 12, o que em símbolos se escreve mdc(8,12)=4 ou (8,12)=4, quando não houver ambigüidade.

Tem-se $m = \text{mdc}(a, b)$ sempre que cumprirem-se as propriedades seguintes:

(i) $m|a$ e $m|b$

(ii) se $d|a$ e $d|b$ então $d|m$

(iii) $m > 0$

A propriedade (i) diz que o mdc de dois números é um divisor comum desses números; (ii) nos diz que todo divisor comum de a e b também divide seu mdc; se m satisfaz (i) e (ii), então $-m$ também satisfaz (i) e (ii), de modo que, para evitar ambigüidade, (iii) nos diz para tomarmos sempre o valor positivo.

Essas questões são fundamentais e precisamos delas para prosseguir. Este é o motivo pelo qual as menciono aqui. Qualquer livro de introdução a Teoria dos Números traz logo no início essas informações.

Inteiros coprimos

Dois números inteiros são ditos *coprimos*, ou *relativamente primos* ou ainda *primos entre si* sempre que seu máximo divisor comum for igual a 1. Assim, 27 e 80 são coprimos, porque mdc(27, 80)=1. Entretanto 48 e 33 não são relativamente primos, uma vez que mdc(48, 33)=3≠1.

Definindo números primos

Os números primos são os números naturais que têm exatamente dois divisores positivos. Esta não é uma definição citada com freqüência, mas é a que me parece, aqui, a mais adequada. Existem outras definições equivalentes. A mais popular diz que número primo é um inteiro maior que 1 cujos únicos divisores positivos são 1 e ele mesmo. Assim, 7 é primo, pois seus únicos divisores são 1 e 7; mas 9 não é primo pois tem três divisores: 1, 3 e 9.

Ainda há uma definição importante de número primo. Ela diz que um inteiro $p>1$ é primo quando $p|a$ ou $p|b$, para *quaisquer* inteiros a e b tais que $p|ab$. Logo, quando um primo divide um produto, necessariamente divide algum dos fatores.

A seqüência dos primos

Os dez primeiros números primos são 2, 3, 5, 7, 11, 13, 17, 19, 23 e 29. Esta lista pode ser estendida indefinidamente, conforme mostraremos ainda neste capítulo. Então, existe uma *sucessão* ou *seqüência* de números primos. Faz sentido, portanto, falar num primeiro número primo, que é o 2; num segundo primo (o 3) e mais geralmente num n-ésimo número primo, que ocupa a posição n na sucessão e é denotado por p_n. Assim, por exemplo, $p_{10} = 29$, ou seja, o décimo primo é 29.

Algumas notações

O conceito de número primo está fortemente ligado ao de *divisibilidade*. Dado um inteiro positivo *n*, seu *número de divisores positivos* é representado por $\mathrm{d}(n)$. Assim, um número natural *p* é primo quando $\mathrm{d}(p)=2$. Por exemplo, os divisores de 127 são 1 e 127; então $\mathrm{d}(127)=2$ e portanto 127 é primo. Por outro lado, os divisores de 128 são 1, 2, 4, 8, 16, 32, 64 e 128 em número de 8; logo $\mathrm{d}(128)=8\neq 2$ e portanto 128 não é primo.

Vimos duas notações: p_n designa o *n*-ésimo primo e $\mathrm{d}(n)$ a quantidade de divisores de *n*. Usaremos essas designações em todo livro. Elas são empregadas com bastante freqüência pelos matemáticos e se consagraram pela tradição. Uma outra função comum em Teoria dos Números é a σ_k. Representa-se por $\sigma_k(n)$ a soma das *k*-ésimas potências dos divisores positivos de *n*. Note o leitor que para qualquer inteiro *n*, tem-se $\sigma_0(n)=\mathrm{d}(n)$. Além disso, denotando por $\mathrm{s}(n)$ a soma dos divisores de *n*, vale $\sigma_1(n)=\mathrm{s}(n)$. Então, pode-se usar uma ou outra notação conforme for conveniente.

Uma primeira fórmula

Já se pode, com o que vimos até aqui, escrever uma fórmula para primos. Basta notar que:

(i) Dado *n*>1, a sucessão $\sigma_{-1}(n),\sigma_{-2}(n),\sigma_{-3}(n),\ldots$ converge para 1;

(ii) A sucessão $\sqrt[-1]{\sigma_{-1}(n)-1},\sqrt[-2]{\sigma_{-2}(n)-1},\sqrt[-3]{\sigma_{-3}(n)-1},\ldots$ converge para o menor divisor maior que 1 de *n*;

(iii) De modo mais geral $\lim\limits_{\alpha\to-\infty}\sqrt[\alpha]{\sigma_\alpha(n)-1}$ é o menor divisor maior que 1 de *n*;

(iv) Dado qualquer inteiro *n*>1, seu menor divisor maior que 1 é primo;

(v) Logo, $f(n)=\lim\limits_{\alpha\to-\infty}\sqrt[\alpha]{\sigma_\alpha(n)-1}$ produz todos os primos, e somente primos sendo, portanto, uma fórmula para primos.

Alguns leitores podem ficar um pouco desapontados com este primeiro exemplo. Para calcular o valor de $f(n)$ é necessário conhecer os divisores n. Mais que isto: é preciso que conheçamos a soma das α-ésimas potências dos divisores de n (quando α tende a $-\infty$ (!)). É muito complicado usar esta fórmula para calcular primos.

Não obstante, ela é bonita! É concisa, não trivial e faz exatamente o que dela se pede: produz (todos os) primos e somente primos, embora de modo computacionalmente ineficaz. Neste livro não nos prenderemos meramente a questão estética das fórmulas. Também serão levantadas questões teóricas, conjecturas sugeridas explicita ou implicitamente. Não é nosso objetivo aqui medir a rapidez das fórmulas ou sua *complexidade computacional*, embora esta questão interesse a muitos matemáticos de renome.

O crivo de Eratóstenes

Se estivéssemos interessados em determinar rapidamente todos os primos menores que um número dado, seria insensato usar a fórmula que vimos. Em vez disso, usaríamos o crivo. Ele consiste num *algoritmo* devido ao matemático grego Eratóstenes (276 a.C–194 a.C), o mesmo que fez a primeira estimativa para a circunferência da Terra. O crivo consiste em, dado um inteiro $n>3$, determinar todos os números primos menores que n mediante as seguintes etapas:

Etapa 1: Escrevemos os números ímpares do intervalo aberto $]2,n[$ em ordem crescente numa tabela;

Etapa 2: Circulamos o menor número não circulado e não cortado (este número é primo);

Etapa 3: Chamamos de c o maior número circulado. Se $n>c^2$ passamos para a etapa 4. Caso contrário encerramos o algoritmo e os números primos menores que n são exatamente aqueles que não foram cortados (os circulados também são primos) e também o inteiro 2.

Etapa 4: Iniciando por c^2, vamos cortando os números da tabela de c em c, isto é, cortamos c^2, c^2+c, c^2+2c etc. (cortamos estes números pois eles não são primos, por serem múltiplos de c; não precisamos cortar nenhum múltiplo de c

menor que c^2 pois eles já foram cortados antes). Nesta etapa é como se estivéssemos *peneirando* nossa tabela de números, por isso o nome *crivo*. Neste momento retorna-se à etapa 2.

O crivo é um meio rápido de decidir quais números menores que um inteiro dado são primos, e quais não são. Os que não são primos se escrevem como produto de primos (com exceção de 1) e por isto chamam-se *compostos*. O número 1 não é considerado nem primo nem composto. É interessante notar que para os gregos antigos 1 não era nem sequer um número (veja p.1 de [15]).

As funções π , teto, chão e parte fracionária

Voltemos ao crivo. Como ele nos mostra todos os primos menores que um inteiro *n*, é natural nos perguntarmos *quantos* primos há até *n*. Representa-se por $\pi(n)$ a quantidade de números primos menores *ou iguais* a *n*. Assim, $\pi(1)=0$ pois não há primos no intervalo $[1,1]=\{1\}$; $\pi(11)=5$, porque no intervalo $[1,11]$ existem 5 números primos, a saber, 2, 3, 5, 7 e 11.

Sabemos que primalidade está relacionada com divisibilidade. E quando nos questionamos a respeito de divisibilidade, estamos procurando informações a respeito de alguma divisão. Por outro lado, números primos são sempre *inteiros*, mas muitos valores de funções *não* são números inteiros. Então precisamos, algumas vezes, "converter" números reais em inteiros. Por isso, duas funções que aparecem com freqüência quando se buscam fórmulas para primos são a *chão* e a *teto*. O chão de *x* é denotado por $\lfloor x \rfloor$ e é o maior inteiro $\leq x$. O teto de *x* é denotado por $\lceil x \rceil$ e é o menor inteiro $\geq x$. Os números $\lfloor x \rfloor$ e $\lceil x \rceil$ são os únicos *inteiros* que satisfazem $x-1<\lfloor x \rfloor \leq x \leq \lceil x \rceil < x+1$. Note que chamar $\lfloor x \rfloor$ de o *chão* de *x* e $\lceil x \rceil$ de o *teto* de *x* está em conformidade com o que é sugerido graficamente por estes símbolos.

Assim, por exemplo, $\lfloor 7,8 \rfloor = 7$ e $\lceil 20,2 \rceil = 21$. Com números negativos tem-se $\lfloor -7,42 \rfloor = -8 = \lceil -8,17 \rceil$. Quando *x* é inteiro, tanto o chão quanto o teto de *x* igualam-se a *x*.

Cabe notar que quando n e d são inteiros positivos, o quociente da divisão do primeiro pelo segundo é $\lfloor n/d \rfloor$.

Uma outra função que ocorre com alguma freqüência é a *parte fracionária*. Ela é denotada e definida por $\{x\} = x - \lfloor x \rfloor$. Para números inteiros esta função se anula; para reais *positivos* ela é muito fácil de calcular: $\{13{,}147\} = 0{,}147 = \{666{,}147\}$ etc.

Uma fórmula de Willans

Já podemos examinar uma segunda fórmula para primos, devida a Willans. É ela:

$$p_n = 1 + \sum_{m=1}^{2^n} \left\lfloor \sqrt[n]{\frac{n}{1+\pi(m)}} \right\rfloor$$

É uma fórmula elegante, sem dúvida. Escreve-se com simplicidade e oculta a magia de sua verdade. Além disso, não dá somente infinitos primos ou todos os primos. Ela faz mais: calcula o n-ésimo número primo.

Ainda assim, é uma idéia muito má calcular primos usando essa fórmula. Para se ter uma idéia do que acontece, basta fazer n=10 e espiar a expressão que obtemos.

$$p_{10} = 1 + \sum_{m=1}^{1024} \left\lfloor \sqrt[10]{\frac{10}{1+\pi(m)}} \right\rfloor$$

O cálculo desta expressão pressupõem o conhecimento de todos os valores de $\pi(m)$ para m entre 1 e 1024=2^{10}. Em particular, precisaríamos conhecer o valor de $\pi(1024)$, que já é muito mais difícil de calcular que o próprio $p_{10} = 29$.

Examinemos a fórmula de Willans. Como ela funciona? A idéia não é difícil de entender. Cada parcela do somatório é igual a 1 quando $m < p_n$ e é igual a 0 se $m \geq p_n$. Assim, no somatório para m de 1 a 1024 há $p_n - 1$ parcelas iguais a 1, sendo nulas as demais. Com a unidade que é adicionada no início da fórmula, o valor da expressão passa a ser exatamente p_n.

Fórmulas correlatas

Aproveitando a idéia da fórmula de Willans, pode-se escrever:

$$p_{n+1} = 2 + \sum_{m=2}^{2+n^2} \left\lfloor \frac{n}{\max\left(n, \pi(m)\right)} \right\rfloor \qquad p_n = 1 + \sum_{m=1}^{n^2} \left\lfloor \frac{n}{\max\left(n, 1+\pi(m)\right)} \right\rfloor$$

$$\begin{cases} p_1 = 2 \\ p_{n+1} = p_n + \sum_{m=p_n}^{1+n^2} \left\lfloor n/\pi(m) \right\rfloor \end{cases} \qquad p_n = 1 + \sum_{m=1}^{n^2} \left\lceil \frac{n-\pi(m)}{\max\left(n, \pi(m)\right)} \right\rceil$$

onde, lembro, $\lceil x \rceil$ denota o menor inteiro maior ou igual a *x*, chamado *teto* de *x*.

O *postulado de Bertrand* e uma cota superior para p_n

Ainda há um ponto não explicado na fórmula de Willans. Porque ele somou para *m* de 1 a 2^n? A razão para isso é que como cada parcela do somatório não excede 1, devem haver pelo menos $p_n - 1$ delas, pois caso contrário a fórmula daria um número menor que p_n. Se somássemos, por exemplo, para *m* de 1 a 2*n*, fazendo *n*=10 já não teríamos o resultado correto $p_{10} = 29$; o somatório seria para *m* de 1 a 20=2×10=2*n* e a fórmula produziria 1+20=21<29. Em outras palavras, precisamos ter no somatório um número de parcelas que seja maior ou igual a $p_n - 1$. Para isso é mais que suficiente que tenhamos $2^n \geq p_n$ parcelas no somatório.

Há um bom argumento para mostrar que $p_n \leq 2^n$. Basta aplicar o *postulado de Bertrand*, que apesar do nome não é um postulado, mas sim uma conjectura provada por Chebyshev em 1852. Este teorema afirma que se *n*>1, então existe algum número primo no intervalo aberto $]n, 2n[$. Logo, existe pelo menos um primo em cada um dos *n*-1 intervalos disjuntos $]2,4[,]4,8[,]8,16[, \ldots \left]2^{n-1}, 2^n\right[$, e portanto há um mínimo de *n*-1 primos no intervalo $\left]2, 2^n\right[$. Como 2 é primo, existem pelo menos *n* números primos no intervalo $\left[2, 2^n\right]$, isto é, $p_n \leq 2^n$.

O teorema de Wilson: congruências e fatorial

O matemático inglês Wilson, no século XVIII, provou um resultado que *caracteriza* os números primos. Dá um critério, ainda que pouco prático, para determinar se um número >1 é primo ou composto. Para enunciar este teorema, é útil conhecer a noção de congruência.

Sejam *a*, *b*, *c* números inteiros. Dizemos que *a* é *congruente b módulo c*, e simbolizamos isto por $a \equiv b \mod c$ quando *a* e *b* tiverem o mesmo resto na divisão por *c*. Ou, de modo equivalente, escrevemos $a \equiv b \mod c$ para significar que *c* divide $a-b$. Um exemplo: $21 \equiv 9 \mod 4$ pois 4|(21-9), isto é, 4|12.

O fatorial de um inteiro *n*>1 é o produto de todos os inteiros positivos até *n* inclusive. Ele é denotado por $n!$ e definido por $n! = 1 \times 2 \times 3 \times \cdots \times n$. Assim, $3! = 1 \times 2 \times 3 = 6$. Define-se também 0!=1!=1.

Wilson demonstrou que um inteiro $n > 1$ é primo se, e somente se, $(n-1)! \equiv -1 \mod n$. Fazendo, por exemplo, *n*=5 tem-se $(5-1)! = 4! = 24 \equiv -1 \mod 5$, logo, conforme o teorema de Wilson, 5 é primo.

Duas fórmulas para primos que utilizam o teorema de Wilson

A primeira é $f(x,y) = \frac{y-1}{2}\left[\left|a^2-1\right| - \left(a^2-1\right)\right] + 2$, onde *x* e *y* são inteiros positivos e $a = x(y+1) - (y!+1)$. Tem-se: $f(1,1) = 2$, $f(1,2) = 3$, $f(5,4) = 5$, $f(103,6) = 7$, $f(329891,10) = 11$, $f(36846277,12) = 13$ e de modo geral para cada primo *p* tem-se $f\left(\frac{(p-1)!+1}{p}, p-1\right) = p$, donde a fórmula produz todos os primos. Usando o teorema de Wilson prova-se que essa fórmula gera *somente* primos. De fato, se $a^2 \geq 1$ então $f(x,y) = 2$ é primo. Se por outro lado *a*=0 então $x(y+1) = (y!+1)$ donde $(y+1) \mid (y!+1)$, isto é, $y! \equiv -1 \mod (y+1)$, e daí, tomando *n*=*y*+1 no teorema de Wilson tem-se que *y*+1 é primo. Ora, este é exatamente o valor de $f(x,y)$ quando *a*=0.

Logo, os valores de $f(x, y)$ são sempre números primos, para cada par x, y de inteiros positivos.

Não se trata de uma fórmula prática, entretanto. Ela tem uma "predileção muito grande pelo número primo 2", como nos observa R. Watanabe em [2]. Além disso, mesmo para produzir primos pequenos, começamos a ter problemas com a magnitude dos números envolvidos. Um exemplo é o cômputo de $p_{10} = 29$, que nos remete ao cálculo de 28!, um número de trinta algarismos.

A segunda fórmula é $f(n) = 2 + ((2n!) \bmod (n+1))$ onde se escreve $a \bmod b$ para denotar o resto da divisão de a por b. Assim, 10 mod 3 = 1 e 23 mod 4 = 3. Notar que $2n!$ é o dobro do fatorial de n, e não o fatorial de $2n$.

Deixo como exercício para o leitor verificar que se n+1 é composto então ele divide $2n!$. Neste caso $(2n!) \bmod (n+1) = 0$ e portanto $f(n) = 2 + ((2n!) \bmod (n+1)) = 2 + 0 = 2$ é primo.

Por outro lado, se n+1 é um número primo então segundo o teorema de Wilson, $n! \equiv -1 \mod (n+1)$. Multiplicando por 2 e desenvolvendo tem-se $2n! \equiv -2 \equiv -2 + (n+1) \equiv n-1 \mod (n+1)$. Portanto n-1 é o resto da divisão de $2n!$ por n+1. Assim, $f(n) = 2 + ((2n!) \bmod (n+1)) = 2 + (n-1) = n+1$ é primo.

Seja n+1 primo ou composto, $f(n)$ é um número primo. Essa fórmula produz primos para todo inteiro não negativo n.

Uma fórmula de Mináč para $\pi(n)$

É ela:

$$\pi(n) = \sum_{i=2}^{n} \left\lfloor \frac{(i-1)!+1}{i} - \left\lfloor \frac{(i-1)!}{i} \right\rfloor \right\rfloor$$

O somatório é para i de 2 até n. Cada vez que i for primo, a respectiva parcela será igual a 1. Caso contrário será igual a zero. Então o valor do somatório será precisamente $\pi(n)$. Deve-se provar, portanto, que

$$(*) \qquad \left\lfloor \frac{(i-1)!+1}{i} - \left\lfloor \frac{(i-1)!}{i} \right\rfloor \right\rfloor = \begin{cases} 1 \text{ se } i \text{ é primo} \\ 0 \text{ se } i \text{ é composto} \end{cases}$$

Se i é primo então pelo teorema de Wilson $(i-1)! \equiv -1 \bmod i$, isto é, $i \mid (i-1)!+1$, ou seja, existe q inteiro satisfazendo $(i-1)!+1 = qi$. Logo, se i é primo,

$$\left\lfloor \frac{(i-1)!+1}{i} - \left\lfloor \frac{(i-1)!}{i} \right\rfloor \right\rfloor = \left\lfloor \frac{qi}{i} - \left\lfloor \frac{qi-1}{i} \right\rfloor \right\rfloor = \left\lfloor q - \left\lfloor q - \frac{1}{i} \right\rfloor \right\rfloor = \lfloor q-(q-1) \rfloor = \lfloor 1 \rfloor = 1$$

Por outro lado, se $i > 5$ é composto então

- ou bem $i = ab$ com $1 < a < b < i$ e $i \mid 1 \times 2 \times \cdots \times a \times \cdots \times b \times \cdots \times (i-1)$;
- ou bem $i = p^2$ é o quadrado de um primo ímpar e $i \mid 1 \times 2 \times \cdots \times p \times \cdots \times 2p \times \cdots \times (i-1)$.

Em qualquer caso $i \mid (i-1)!$, isto é, existe um inteiro q satisfazendo $(i-1)! = qi$ donde:

$$\left\lfloor \frac{qi+1}{i} - \left\lfloor \frac{qi}{i} \right\rfloor \right\rfloor = \left\lfloor q + \frac{1}{i} - q \right\rfloor = \left\lfloor \frac{1}{i} \right\rfloor = 0$$

O caso i=4 é tratado separadamente e não oferece problema:

$$\left\lfloor \frac{3!+1}{4} - \left\lfloor \frac{3!}{4} \right\rfloor \right\rfloor = 0$$

Fica assim provada a relação (*) e também a fórmula de Minác.

Os números de Fermat

O matemático amador francês Pierre de Fermat (1601-1665) acreditava que todos os números da forma $F_n = 2^{2^n} + 1$ fossem primos, para todo inteiro não negativo *n*. Os números que têm essa forma são conhecidos hoje em dia como *números de Fermat*.

Se todo número de Fermat fosse primo teríamos uma fórmula bastante sucinta e elegante que nos retornaria uma infinidade de primos. É claro que isto tiraria a maior parte do interesse no tema deste livro. Felizmente, ou infelizmente, nem todo número de Fermat é primo. De fato:

$$F_0 = 2^{2^0} + 1 = 3 \text{ é primo}$$
$$F_1 = 2^{2^1} + 1 = 5 \text{ é primo}$$
$$F_2 = 2^{2^2} + 1 = 17 \text{ é primo}$$
$$F_3 = 2^{2^3} + 1 = 257 \text{ é primo}$$
$$F_4 = 2^{2^4} + 1 = 65537 \text{ é primo, porém...}$$
$$F_5 = 2^{2^5} + 1 = 4.294.967.297 = 641 \times 6.700.417 \text{ é composto}$$

Note que F_5 é suficientemente grande para inibir a verificação de sua primalidade pelas técnicas disponíveis naquele tempo. Não obstante, Leonhard Euler (1707-1783) fatorou F_5 no ano de 1732, confirmando sua incrível habilidade para cálculos.

Se F_n é primo ele é chamado de *primo de Fermat*. São conhecidos apenas cinco primos de Fermat e atualmente sabe-se que F_n é composto para n = 5, 6, 7, ..., 16 além de outros valores. Isto refutou completamente a conjectura de Fermat e fez com que os matemáticos se perguntassem se existe apenas um número finito de primos de Fermat, ou mesmo apenas cinco.

Custa-nos supor que um matemático do porte de Fermat tenha feito uma conjectura baseando-se tão somente no exame de apenas cinco casos. O fato dos primeiros cinco números que levam seu nome serem primos é um indício muito fraco para se afirmar que *todo*s os outros também são. Ele pode ter tido uma razão mais forte para fazer sua conjectura. Antes de tentar explicar isso, algumas propriedades interessantes dos números de Fermat devem ser mencionadas:

(i) $F_0 F_1 F_2 \cdots F_n = F_{n+1} - 2$

(ii) Se $n \neq m$ então $\text{mdc}(F_n, F_m) = 1$

(iii) $F_n \mid 2^{F_n} - 2$

Alguns comentários: o item (i) prova-se por indução; (ii) pode ser provado a partir de (i); para provar (iii) um bom caminho é usar congruências. Note que (ii) acarreta a existência de uma infinidade de números primos. De fato, sendo os números de Fermat dois a dois coprimos, em cada um deles comparece algum fator primo que não está em nenhum dos demais.

Voltemos à razão de Fermat para fazer sua conjectura. Havia uma hipótese chinesa que dizia que o inteiro $n > 1$ é primo se, e só se, n divide 2^n-2. Sabe-se hoje em dia que isto é falso, pois Sarrus mostrou que 341 divide 2^{341}-2, entretanto 341=31×11 não é primo. Mas naquela época Fermat não conseguiu um contra-exemplo para a hipótese chinesa. Se admitirmos que ele provou a propriedade (iii), o que é bem possível, e juntarmos a isto a hipótese chinesa, a conseqüência imediata é a primalidade de F_n. Esta explicação para a motivação de Fermat foi sugerida pelo astrônomo polonês Banachiewicz.

Vale a pena mencionar que Carl Friedrich Gauss (1777-1855) relacionou os números de Fermat ao problema da ciclotomia, isto é, a divisão da circunferência em partes iguais, realizada com régua e compasso. Gauss mostrou que a divisão é possível se, e só se, o número n de partes for uma potência de 2 ou o produto de uma potência de 2 por distintos *primos* de Fermat.

Finalmente, o leitor deve notar que com sua conjectura Fermat estava, essencialmente, propondo uma fórmula para primos. Ora, se o grande matemático que foi Fermat propôs uma fórmula para primos, isto é suficiente para validar o interesse no tema. Por outro lado, tendo ele falhado em sua fórmula, isto nos mostra a dificuldade do assunto.

2

Uma Função de Variável Matricial que Produz Números Primos

Introdução

Os números primos desafiam há muito tempo a engenhosidade e a imaginação do ser humano. Muitas questões interessantes podem ser levantadas, no que diz respeito à distribuição, reconhecimento e geração de números primos. Não são poucos os professores e estudantes de Matemática que desconhecem a existência de funções que geram números primos. Por outro lado, existem muitos resultados nesse sentido.

A idéia central do presente trabalho não é nova. Trata-se de uma generalização dos argumentos que Euclides (séc. III a.C.), Stieltjes (1856-1894), e Métrod (em 1917) usaram em suas demonstrações de que o conjunto dos números primos é infinito (veja [4]). Basicamente essas demonstrações partem de um conjunto C de números primos para construir um número $P > 1$ que é relativamente primo com cada número em C. Então P admite algum fator primo que não está em C. Sob certas condições pode-se afirmar que P é primo.

Produzindo primos: uma receita

Dado um inteiro $t > 1$, sejam $q_1, q_2,..., q_n$ inteiros positivos satisfazendo:

(i) $\text{mdc}(q_i, q_j) = 1$ sempre que $i \neq j$;

(ii) $q_1 q_2 \ldots q_n$ é divisível por cada número primo menor que t.

Sejam m inteiros positivos $b_1, b_2,..., b_m$ tais que

(iii) cada b_i pode ser escrito como o produto de potências dos números $q_1, q_2,..., q_n$ com expoentes inteiros não negativos;

(iv) para cada $j = 1, 2, ..., n$, exatamente um entre os b_i's não é divisível por q_j;

Seja ainda $s_i \in \{1, -1\}$, $i = 1, 2, ..., m$. Não é difícil ver que $\Sigma s_i b_i$ é relativamente primo com $q_1 q_2 \cdots q_n$. De fato, se p é primo e $p \mid q_1 q_2 \cdots q_n$, então pela condição (i) p divide *exatamente um* entre os q_i's, digamos, q_1; mas pela condição (iv), $\Sigma s_i b_i$ é uma soma em que *exceto uma, todas* as parcelas são divisíveis por q_1, e também por p. Logo $\Sigma s_i b_i$ não é divisível por p nem por nenhum primo menor que t.

Seja M um múltiplo de todos os primos menores que t e $P = |M + \Sigma s_i b_i|$. Como P é o módulo da soma de um número que é divisível por cada primo menor que t, com um número que não é divisível por nenhum primo menor que t, então P não é divisível por nenhum primo menor que t.

Se P é composto, certamente ele não é menor que t^2, pois todo natural composto menor que t^2, admite algum fator primo menor que t, o que não é o caso de P. Portanto, se $1<P<t^2$ então P será um número primo.

Se quisermos uma fórmula para primos consideramos a função h que terá valor P, caso P seja maior que 1 e menor que t^2, e valor 2 caso contrário. A imagem de h é um conjunto de números primos. Por outro lado, seja qual for o valor de P várias questões podem ser levantadas a seu respeito.

Dois modos de escolher os q_i's

Pode-se escolher n-uplas q satisfazendo as condições (i) e (ii) de muitos modos. Mostrarei dois.

Primeiro modo

Sejam $q_1, q_2,..., q_{n-1}$ primos distintos e $t > 1$ um número natural.

Lema. *Seja p primo, m inteiro positivo e* $p^k \le m < p^{k+1}$. *O expoente da maior potência de p que divide m! é*:

$$\left\lfloor \frac{m}{p} \right\rfloor + \left\lfloor \frac{m}{p^2} \right\rfloor + \left\lfloor \frac{m}{p^3} \right\rfloor + \cdots + \left\lfloor \frac{m}{p^k} \right\rfloor = \sum_{c \text{ natural}}^{1 < p^c \le m} \left\lfloor \frac{m}{p^c} \right\rfloor$$

onde $\lfloor x \rfloor$ é o maior inteiro menor ou igual a x. Em [4] e em [6] encontramos uma justificativa para o lema. Aplicando-o teremos o expoente inteiro da maior potência do primo q_j que divide $(t-1)!$, e também o produto Q dessas potências, donde $q_n = (t-1)!/Q$ é um possível valor para o n-ésimo termo de uma n-upla q satisfazendo as condições (i) e (ii). De fato, q_n é relativamente primo com q_1, q_2, ..., q_{n-1} e no produto $q_1 q_2 ... q_n$ comparecem todos os fatores primos de $(t-1)!$. Portanto, as condições (i) e (ii) são satisfeitas.

Segundo modo

Faça $q_n = \dfrac{(2n)!}{\text{mdc}\left((2n)!, (2n-2)!^3\right)}$. Não é difícil verificar que

$$q_n = \begin{cases} 2 & \text{se } n = 1 \\ 2n-1 & \text{se } 2n-1 \text{ é primo} \\ 1 & \text{nos outros casos} \end{cases}$$

donde as condições (i) e (ii) ficam satisfeitas. Note que a função $g(n) = \max(2, q_n)$ já é, por si mesma, uma fórmula para primos.

Definindo matrizes adequadas: calculo dos b_i´s

Direi que uma matriz $A \in M_{m \times n}(\mathbb{Z})$ com termos não negativos é *adequada* quando cada uma de suas colunas tiver exatamente um termo nulo. Seja $A = (a_{ij})$ uma m por n matriz adequada e $s = (s_1, s_2, ..., s_m)$ onde $s_i \in \{-1, 1\}$ para $i = 1, 2, 3, ..., m$. É fácil ver que se

$$b_i = \prod_{j=1}^{n} q_j^{a_{ij}} \text{ para } i = 1, 2, \ldots, m$$

então os inteiros b_i's acima definidos cumprem as condições (iii) e (iv).

A matriz euclidiana

Dado um inteiro w qualquer e uma n-upla q, chamar-se-à de *matriz euclidiana* a matriz em blocos:

$$E = \left[\begin{array}{c|cccc} w & q_1 & q_2 & \cdots & q_n \\ \hline s_1 & a_{11} & a_{12} & \cdots & a_{1n} \\ s_2 & a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ s_m & a_{m1} & a_{m2} & \cdots & a_{mn} \end{array}\right]$$

onde $A=(a_{ij})$ é matriz adequada; $s_i \in \{1, -1\}$; $w \in \mathbb{Z}$; os q_i's são dois a dois relativamente primos. A função f que nos interessa é dada por

$$f(E) = \left| w\prod_{j=1}^{n} q_j + \sum_{i=1}^{m} s_i \prod_{j=1}^{n} q_j^{a_{ij}} \right|$$

onde E é matriz euclidiana. Outra função que apresenta interesse é dada por

$$g(E) = \min\left(\mathbb{Z} \cap \bigcup_{n \in \mathbb{N}^*} \left\{ \sqrt[n]{f(E)} \right\} \right)$$

Duas fórmulas para primos

Se $1 < P = f(E) < t^2$ (respectivamente $1 < P = g(E) < t^2$) então certamente P é primo. Caso contrário, P pode ou não ser primo. Se $1 < P < t^2$ (t é um inteiro tal que em Πq_i comparecem todos os fatores primos menores que t) tome $h(E) = f(E)$

(respectivamente $h(E)=g(E)$); se $P = 1$ ou $P \geq t^2$ faça $h(E)=2$. Deste modo $h(E)$ é sempre um número primo. Eis aí dois exemplos de fórmulas para primos.

Exemplos

O conjunto das matrizes euclidianas é o domínio onde está definida nossa função *f*. Por exemplo:

$$f\begin{pmatrix} 0 & 2 & 3 & 5 & 7 \\ 1 & 3 & 2 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 \end{pmatrix} = 107$$

uma vez que 0×2×3×5×7+2^3×3^2×5^0×7^0+2^0×3^0×5^1×7^1=107. Note que t=11 já que escolhemos $q_1 = 2, q_2 = 3, q_3 = 5, q_4 = 10!/(2^8 3^4 5^2) = 7$, conforme o *primeiro modo*. Isto significa que no produto $q_1 q_2 q_3 q_4$ comparecem todos os fatores primos menores que t = 11. Como 107 < 11^2, tem-se que 107 é primo. Outro exemplo é o seguinte

$$f\begin{pmatrix} 87 & 2 & 3 & 5 & 77 \\ 1 & 7 & 0 & 3 & 0 \\ -1 & 2 & 2 & 0 & 2 \\ -1 & 0 & 2 & 1 & 1 \end{pmatrix} = 61$$

onde $q_1 = 2, q_2 = 3, q_3 = 5, q_4 = 11!/(2^8 3^4 5^2) = 77$ foram escolhidos do *primeiro modo*.

A infinitude dos primos e as matrizes euclidianas

Suponha por absurdo que exista apenas um número finito de primos, sejam eles, $p_1, p_2, ..., p_r$. Euclides chegou a uma contradição considerando o número $P_E = p_1 p_2 \cdots p_r + 1$. De fato, algum primo p_i divide P_E, pois todo inteiro é divisível por algum primo, logo $p_i \mid P_E - p_1 p_2 \cdots p_i \cdots p_r \Rightarrow p_i \mid 1$, absurdo. Isto equivale a considerar a matriz euclidiana

$$E=\left(\begin{array}{c|cccc} 0 & p_1 & p_2 & \cdots & p_r \\ \hline 1 & 1 & 1 & \cdots & 1 \\ 1 & 0 & 0 & \cdots & 0 \end{array}\right) \text{ ou } E=\left(\begin{array}{c|cccc} 1 & p_1 & p_2 & \dots & p_r \\ \hline 1 & 0 & 0 & \dots & 0 \end{array}\right)$$

e concluir que existe um primo diferente de $p_1, p_2, ..., p_r$, a saber, qualquer fator primo de $f(E)$.

Stieltjes usou uma idéia similar. Ele considerou o número $P_S=m+n$ onde m,n são inteiros satisfazendo $mn = p_1 p_2 \cdots p_r$. Note que mdc(m, n)=1, logo mdc(mn, $m+n$) = 1. Portanto existe algum primo diferente de $p_1, p_2, ..., p_r$, a saber, qualquer fator primo de $m+n$. Eis o absurdo, pois por hipótese não havia outros primos senão $p_1, p_2, ..., p_r$. Isto equivale a considerar a matriz euclidiana

$$S=\left(\begin{array}{c|cccc} 0 & p_1 & p_2 & \cdots & p_r \\ \hline 1 & m_1 & m_2 & \dots & m_r \\ 1 & n_1 & n_2 & \dots & n_r \end{array}\right)$$

onde para cada i = 1, 2, ..., r, ou m_i = 1 e n_i = 0, ou m_i = 0 e n_i = 1, isto é, os elementos da matriz adequada correspondente são zeros e uns. Nenhum fator primo de $f(S)$ está na lista $p_1, p_2, ..., p_r$, e aí reside o absurdo.

A demonstração de Métrod para a infinitude dos primos considera matrizes euclidianas com mais de três linhas. Seja $N = p_1 p_2 \cdots p_r$, $Q_i = N/p_i$ e $P_M = \sum_{i=1}^{r} Q_i$. Como p_i divide Q_j (para $i \neq j$) e p_i não divide Q_i, então p_i não divide P_M. Logo nenhum dos primos $p_1, p_2, ..., p_r$ divide P_M: absurdo. Isso equivale a considerar a matriz euclidiana

$$M=\left(\begin{array}{c|ccccc} 0 & p_1 & p_2 & p_3 & \cdots & p_r \\ \hline 1 & 0 & 1 & 1 & \dots & 1 \\ 1 & 1 & 0 & 1 & \dots & 1 \\ 1 & 1 & 1 & 0 & \dots & 1 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & 1 & 1 & \dots & 0 \end{array}\right)$$

em que a diagonal principal é formada por zeros somente e os outros elementos da matriz adequada correspondente são iguais a 1.

Indícios empíricos e conjecturas

Sejam $N = p_1 p_2 \cdots p_r$, $Q_i = N/p_i$, $s_i \in \{1,-1\}$ e $P'_M = \sum_{i=1}^{r} s_i Q_i$. Pode ser verificado com um sistema de computação algébrica que para cada r=2,3,4,...,149, existe alguma r-upla $(s_1, s_2, \ldots, s_r) \in \{1,-1\}^r$ tal que P'_M é um número primo. É lícito conjecturar, portanto:

$$f\begin{pmatrix} 0 & p_1 & p_2 & p_3 & \cdots & p_r \\ \hline \pm 1 & 0 & 1 & 1 & \cdots & 1 \\ \pm 1 & 1 & 0 & 1 & \cdots & 1 \\ \pm 1 & 1 & 1 & 0 & \cdots & 1 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ \pm 1 & 1 & 1 & 1 & \cdots & 0 \end{pmatrix}$$

é um número primo para cada $r > 1$ e alguma escolha conveniente entre +1 e -1 na primeira coluna da matriz euclidiana.

Ainda com um sistema de computação algébrica pode-se verificar que para r=2,3,4,...,144, é suficiente tomar *todas, exceto no máximo duas* parcelas do somatório $P'_M = \sum_{i=1}^{r} s_i Q_i$ negativas para que P'_M seja um primo. Estes indícios experimentais nos levam a uma conjectura mais forte que a anterior: se N é o produto dos n primeiros números primos e $Q_i = N/p_i$ então ou a soma $\sum Q_i$ é um número primo, ou se trocarmos o sinal de algum Q_i, a soma $\sum Q_i$ passa a ser um número primo (isso não funciona para n=44, 53, 67, 93, 96, 98, 120, 128, 132, 141,...) ou trocando o sinal de dois Q_i's, a soma será um número primo. Por exemplo, para n=2, 2+3=5 é primo; para n = 3, 2×3+2×5+3×5=31 é primo; para n=4, 2×3×5+2×3×7+2×5×7-3×5×7=37 também primo. Para n=44, 53, 67 etc precisamos trocar o sinal de dois Q_i's para obter um primo.

As evidências experimentais (verificou-se para $4<n\leq 15$) indicam que cada número primo p satisfazendo $p_{n+1} \leq p < p_{n+1}^2$ é fator de alguma $f(B_q)$, onde $q=(p_1, p_2,..., p_n)$, $n > 4$ e B_q é uma matriz euclidiana com matriz adequada correspondente formada só por zeros e uns.

3

Funções que Geram Números Primos

Introdução

Os números primos fascinam muitos dos que estudam Matemática. Um dos motivos é que o conceito de número primo surge cedo na vida do estudante e, sendo muito fácil definir o que são números primos, é difícil encontrar funções que os gerem. Por outro lado algumas funções que produzem números primos tem sido obtidas por matemáticos como Willans, Ernvall, Sierpinski, Gandhi entre outros. O problema de obter funções que geram números primos já despertou, portanto, o interesse de vários matemáticos.

No presente trabalho estudamos funções $z_m(n)$ que satisfazem

$$n \text{ é primo } \Leftrightarrow n \text{ não divide } z_m(n)$$

A partir daí deduzimos fórmulas para primos e para $\pi(n)$.

Caracterizando Números Primos

Fixado um certo inteiro positivo m, seja

$$\mathrm{N}_m = \{n \in \mathbb{N} \mid n \perp m!\}$$

onde a notação $a \perp b$ significa que mdc(a, b) = 1. Seja ainda (n_i) a sucessão crescente formada pelos elementos de N_m. Note que $n_1 = 1$ e n_2 é o menor número primo maior que m. Será útil definir o mmc de um único inteiro positivo como ele próprio, isto é, mmc(n) = n. Considere a função $z_m : \mathrm{N}_m \to \mathbb{N}$ tal que

$$z_m\left(n_j\right) = \text{mmc}\left\{n_i \in \text{N}_m \mid i \leq j \text{ e } n_i \text{ não é primo}\right\}$$

Gostaríamos de provar que n_j é primo se e somente se n_j não divide $z_m(n_j)$. Fazendo isso teremos uma caracterização dos números primos que pertencem a N_m.

Se n_j não é primo é claro que $n_j \in \left\{n_i \in \text{N}_m \mid i \leq j \text{ e } n_i \text{ não é primo}\right\}$, e portanto n_j divide $z_m(n_j)$. Logo se n_j não divide $z_m(n_j)$ então n_j é primo.

Mostraremos agora que se n_j é primo então n_j não divide $z_m(n_j)$. Suponha que n_j é primo. Nesse caso n_j não divide nenhum produto de inteiros positivos menores que n_j. Como $z_m(n_j)$ pode ser escrito como um produto de inteiros positivos menores que n_j, então n_j não divide $z_m(n_j)$. Logo, se n_j é primo então n_j não divide $z_m(n_j)$.

Ficou provado que n_j é primo se e só se n_j não divide $z_m(n_j)$, e isto caracteriza os números primos que pertencem a N_m. Portanto, se N pode ser fatorado como produto de inteiros menores que n_j, então n_j é primo se e somente se n_j não divide $Nz_m(n_j)$.

Note que $i \leq j$ acarreta $z_m(n_i) | z_m(n_j)$ pois enquanto $z_m(n_i)$ é o mmc de um conjunto de números C, $z_m(n_j)$ é o mmc de um conjunto de inteiros que contém o conjunto C.

O Cálculo de $z_m(n_j)$ e a caracterização dos primos em N_m

Seja $S = S\left(n,m\right) = \left\{s \in \mathbb{Z} \mid 1 \leq s \leq n \text{ e } s \perp m! \text{ e } s \text{ não é primo}\right\}$, $z = z_m\left(n\right) = \text{mmc}\left\{s \mid s \in S\right\}$, $n = n_j$ e $q = n_2$ o menor número primo maior que m. Mostrarei que nenhum primo p satisfazendo $pq>n$ ou $p<q$ divide z. Se $p<q$ então $p \leq m$ e portanto p não divide nenhum elemento de S, donde p não divide z.

Suponha que $p \geq q$. Como pq é o menor número composto em $\text{N}_m \supset S$ que é divisível por p, se $n < pq$ não há nenhum elemento em $S = S\left(n,m\right)$ divisível por p e portanto p não divide z. Ficou provado que se p é primo satisfazendo $n < pq$ ou $p < q$ então p não divide z. Logo, se p divide z então $q^2 \leq pq \leq n$.

Suponha $q^2 \leq pq \leq n$. Como nenhum elemento de S é maior que n, se $n < p^2$ então todo elemento de S é menor que p^2 e p^2 não divide nenhum $s \in S$. Por outro lado, p divide $pq \in S$, logo p^1 é a maior potência de p que divide z. Se $p^2 \leq p^b \leq n < p^{b+1}$, com b inteiro positivo, p^{b+1} não divide nenhum $s \in S$, pois todo elemento de S é menor

ou igual a $n < p^{b+1}$. Mas p^b divide $p^b \in S$, logo p^b é a maior potência de p que divide z. De qualquer modo o expoente inteiro da maior potência de p que divide z é $\lfloor \log_p n \rfloor$. Isto é, a maior potência de p que divide z é a maior potência de p menor ou igual a n. Portanto

$$z_m(n) = \prod_{p \text{ primo}}^{q^2 \le pq \le n} p^{\lfloor \log_p n \rfloor}$$

onde adotamos a convenção $\prod_{q \in \varnothing} q = 1$ (produto vazio). Chegamos ao seguinte

Teorema 1. *Sejam m, n inteiros positivos satisfazendo* $n \perp m!$, *q o menor número primo maior que m, e N um produto qualquer de inteiros positivos menores que n. São equivalentes:*

(i) *n é um número primo*

(ii) *n não divide* $N \prod_{p \text{ primo}}^{q^2 \le pq \le n} p^{\lfloor \log_p n \rfloor}$

onde $p^{\lfloor \log_p n \rfloor}$ *é a maior potência inteira de p menor ou igual a n e* $\Pi_{q \in \varnothing}\, q = 1$.

Corolário 1.1. *Sejam l, m, n inteiros positivos satisfazendo* $n \perp m!$ *e* $n \le l < nq$, *onde q é o menor número primo maior que m e N um produto qualquer de inteiros positivos menores que n. São equivalentes:*

(i) *n é um número primo*

(ii) *n não divide* $N \prod_{p \text{ primo}}^{q^2 \le pq \le l} p^{\lfloor \log_p l \rfloor}$

De fato, como $n \le l$, $z_m(n)$ divide $z_m(l)$. Portanto, se n não é um número primo então n divide $z_m(l)$. Por outro lado, se n é primo e se $n \le l < nq$ então $z_m(l)$ é um produto de primos menores que n, donde n não divide $z_m(l)$.

Corolário 1.2. *Sejam l, m, n inteiros positivos satisfazendo* $n \perp m!$ *e* $n \le l < nq$, *onde q é o menor número primo maior que m. Sejam ainda M um produto qualquer de inteiros positivos menores que n e T um teste de primalidade, um algoritmo que tenha por entrada um inteiro b≥q e diga algo sobre a primalidade de b. Direi que T(b) = 0 se o algoritmo T provar que b é, com certeza, um número composto; e direi que T(b) = 1 nos outros casos. São equivalentes:*

(i) *n* é primo

(ii) *n* não divide $M\prod_{b=q}^{l/q} b^{T(b)\lfloor \log_b l \rfloor}$

A demonstração segue de uma escolha adequada de *N* no corolário 1.1.

Na tabela abaixo vemos que para cada m = 1, 2, 3, 5 e cada i=1,2,...,25, n_i é primo se e só se n_i não divide $z_m(n_i)$. Isso exemplifica o Teorema 1 para N = 1.

	$m = 1$		$m = 2$		$m = 3$		$m = 5$	
i	n_i	$z_1(n_i)$	n_i	$z_2(n_i)$	n_i	$z_3(n_i)$	n_i	$z_5(n_i)$
1	1	1	1	1	1	1	1	1
2	2	1	3	1	5	1	7	1
3	3	1	5	1	7	1	11	1
4	4	4	7	1	11	1	13	1
5	5	4	9	9	13	1	17	1
6	6	12	11	9	17	1	19	1
7	7	12	13	9	19	1	23	1
8	8	24	15	45	23	1	29	1
9	9	72	17	45	25	25	31	1
10	10	360	19	45	29	25	37	1
11	11	360	21	315	31	25	41	1
12	12	360	23	315	35	175	43	1
13	13	360	25	1575	37	175	47	1
14	14	2520	27	4725	41	175	49	49
15	15	2520	29	4725	43	175	53	49
16	16	5040	31	4725	47	175	59	49
17	17	5040	33	51975	49	1225	61	49
18	18	5040	35	51975	53	1225	67	49
19	19	5040	37	51975	55	13475	71	49
20	20	5040	39	675675	59	13475	73	49
21	21	5040	41	675675	61	13475	77	539
22	22	55440	43	675675	65	175175	79	539
23	23	55440	45	675675	67	175175	83	539
24	24	55440	47	675675	71	175175	89	539
25	25	277200	49	4729725	73	175175	91	7007

Duas fórmulas

Sejam $\lfloor x \rfloor$ e $\lceil x \rceil$ o chão e o teto de *x*, definidos como os únicos inteiros tais que $x-1<\lfloor x \rfloor \le x \le \lceil x \rceil < x+1$. Tomando *m*=*N*=1 no teorema 1 tem-se o

corolário 1.3. Seja *n* um inteiro positivo. Então *n* é primo se, e só se, *n* não divide $R_1 = \prod_{p \le n/2}^{p \text{ primo}} p^{\lfloor \log_p n \rfloor}$.

Portanto

$$[\mathrm{A}] \qquad \left\lceil \frac{R_1}{n} \right\rceil - \left\lfloor \frac{R_1}{n} \right\rfloor = \begin{cases} 1, & \text{se } n \text{ é primo} \\ 0, & \text{caso contrário} \end{cases}$$

Por outro lado, tomando $l=n$ e $m=M=T(b)=1$ no corolário 1.2, tem-se o

Corolário 1.4. Seja n um inteiro positivo. Então n é primo se e só se n não divide $R_2 = \prod_{b=2}^{n/2} b^{\lfloor \log_b n \rfloor}$.

Portanto

$$[\mathrm{B}] \qquad \left\lceil \frac{R_2}{n} \right\rceil - \left\lfloor \frac{R_2}{n} \right\rfloor = \begin{cases} 1, & \text{se } n \text{ é primo} \\ 0, & \text{caso contrário} \end{cases}$$

Donde, conforme [A] e [B], para i=1,2 as funções

$$f_i(n) = 2 + (n-2)\left(\left\lceil \frac{R_i}{n} \right\rceil - \left\lfloor \frac{R_i}{n} \right\rfloor\right)$$

produzem todos os primos e apenas primos. De fato se n não é primo, $f(n)=2$; mas se n é primo, então $f(n)=n$.

Um teorema correlato

Temos investigado funções z tais que dado n no domínio de z, n é primo se e só se não divide $z(n)$. Examinaremos agora outros exemplos de funções que satisfazem a esta propriedade e as fórmulas correspondentes para $\pi(n)$ e p_n.

Proposição 1. *Um inteiro* $n \geq 10$ *é primo se e somente se n não divide* $\lfloor n/2 \rfloor !$.

Prova. Se n é primo é claro que n não divide $\lfloor n/2 \rfloor !$. Suponha que n é composto. Se n pode ser escrito como produto de inteiros distintos maiores que 1 acabou, pois cada um

desses fatores distintos é menor ou igual a $\lfloor n/2 \rfloor$, donde n divide $\lfloor n/2 \rfloor !$. Se n não pode ser escrito como produto de inteiros distintos maiores que 1 então $n = p^2$ para algum número primo p. Daí e como $n \geq 10$ por hipótese, vale $4 < p$, donde $2p < p^2/2$, isto é, $2p < n/2$, portanto $p < 2p \leq \lfloor n/2 \rfloor$ e $n = p^2$ divide $\lfloor n/2 \rfloor !$.

Proposição 2. *Um inteiro positivo n é primo se e somente se n não divide $\lfloor n/2 \rfloor ! + 2\delta_{n4} + 3\delta_{n9}$*

Prova. O caso $n \geq 10$ é a proposição 1. Para $n < 10$ a proposição 2 pode ser verificada caso a caso.

Portanto para qualquer inteiro positivo j vale:

$$\left\lceil \frac{R_3}{j} \right\rceil - \left\lfloor \frac{R_3}{j} \right\rfloor = \begin{cases} 1, & \text{se } j \text{ é primo} \\ 0, & \text{caso contrário} \end{cases}$$

logo $\pi(n) = \sum_{j=1}^{n} \left(\left\lceil \frac{R_3}{j} \right\rceil - \left\lfloor \frac{R_3}{j} \right\rfloor \right)$

Três funções para o *n*-ésimo primo

Seja $f(i,n) = \max(\text{sgn}(n - \pi(i)), 0)$. É fácil ver que $f(i,n) = 1$ se $i < p_n$ e $f(i,n) = 0$ se $i \geq p_n$. Se α é uma função que satisfaz $\alpha(n) \geq p_n$ para todo inteiro positivo n, por exemplo, $\alpha(n)=2+2n\log n$, então $p_n = 1 + \sum_{i=1}^{\alpha(n)} f(i,n)$, isto é:

$$p_n = 1 + \sum_{i=1}^{\lfloor 2+2n\log n \rfloor} \max\left(\text{sgn}\left(n - \sum_{j=1}^{i} \left\lceil \frac{R_t}{j} \right\rceil + \sum_{j=1}^{i} \left\lfloor \frac{R_t}{j} \right\rfloor \right), 0 \right)$$

onde R_t, com t=1,2,3, é dado como anteriormente; p_n é o n-ésimo número primo; $\max(u,v) = (u + v + |u - v|) / 2$ é o máximo entre os números u e v.

4

Quatro Fórmulas Relacionadas que Produzem Números Primos

Idéias iniciais

Sejam $\lfloor x \rfloor$ e $\lceil x \rceil$ o chão e o teto de x respectivamente. Os números $\lfloor x \rfloor$ e $\lceil x \rceil$ são os únicos inteiros que satisfazem $x-1<\lfloor x \rfloor \le x \le \lceil x \rceil < x+1$. As igualdades $\lfloor x \rfloor = x = \lceil x \rceil$ somente ocorrem se x é inteiro. Caso contrário, $\lceil x \rceil - \lfloor x \rfloor = 1$. Logo

$$\left\lceil \frac{k}{n} \right\rceil - \left\lfloor \frac{k}{n} \right\rfloor = \begin{cases} 0 & \text{se } n \text{ divide } k \\ 1 & \text{se } n \text{ não divide } k \end{cases}$$

Também é fácil mostrar que $-\lfloor x \rfloor = \lceil -x \rceil$

O produto vazio

O produtório $\prod_{m=a}^{b}(\ldots)$ para $b<a$ e qualquer expressão entre parênteses é chamado de *produto vazio,* uma vez que nele não comparecem fatores. Tem-se $\prod_{m=a}^{b}(\ldots)=1$ pois o produto de "número nenhum" tem o hábito de ser =0, como em $x^0 = 1$ ou em 0! = 1. Um bom argumento neste sentido é a série de Taylor para exp(0):

$$\exp(x) = \sum_{n=0}^{\infty} \frac{x^n}{n!} \text{ logo, } 1 = \exp(0) = \frac{0^0}{0!} + \frac{0^1}{1!} + \frac{0^2}{2!} + \ldots = 0^0$$

Daí, valem as igualdades

$$\prod_{m=a}^{b}(\ldots) = \prod_{m}^{a \le m \le b}(\ldots) = \prod_{m \in \varnothing}(\ldots) = 1 \text{ sempre que } b<a.$$

Fórmula 1. *Seja f a função dada por:*

$$f(n) = -\left\lfloor \log_2 \sum_{k=n+1}^{2n} \frac{1}{2^k} \prod_{m=2}^{n} \left(\left\lceil \frac{k}{m} \right\rceil - \left\lfloor \frac{k}{m} \right\rfloor \right) \right\rfloor$$

então f(*n*) *é o menor número primo maior que n. Além disso,*

$$f(n) = \left\lceil \log_{1/2} \sum_{k=n+1}^{2n} \frac{1}{2^k} \prod_{m=2}^{n} \left(\left\lceil \frac{k}{m} \right\rceil - \left\lfloor \frac{k}{m} \right\rfloor \right) \right\rceil$$

Prova. Se $n = 1$ então $\prod_{m=2}^{n} (\ldots) = 1$, portanto

$$f(1) = -\left\lfloor \log_2 \sum_{k=2}^{2} \frac{1}{2^k} \prod_{m=2}^{1} \left(\left\lceil \frac{k}{m} \right\rceil - \left\lfloor \frac{k}{m} \right\rfloor \right) \right\rfloor = -\left\lfloor \log_2 \frac{1}{2^2} \right\rfloor = 2$$

Assim, para $n = 1$ a função f retorna o menor primo maior que n, sendo a proposição verdadeira neste caso. Suponha $n \geq 2$. Seja k um inteiro no intervalo $(n, 2n]$. Se k é composto ele tem um divisor $d \in [2, n]$, donde

$$\left\lceil \frac{k}{d} \right\rceil - \left\lfloor \frac{k}{d} \right\rfloor = 0 \quad \text{e assim} \quad \prod_{m=2}^{n} \left(\left\lceil \frac{k}{m} \right\rceil - \left\lfloor \frac{k}{m} \right\rfloor \right) = 0$$

Se k é primo, então para todo inteiro $m \in [2, n]$ vale:

$$\left\lceil \frac{k}{m} \right\rceil - \left\lfloor \frac{k}{m} \right\rfloor = 1 \quad \text{e portanto} \quad \prod_{m=2}^{n} \left(\left\lceil \frac{k}{m} \right\rceil - \left\lfloor \frac{k}{m} \right\rfloor \right) = 1$$

Ficou provado que se $2 \leq n < k \leq 2n$ então:

$$g(k, n) = \prod_{m=2}^{n} \left(\left\lceil \frac{k}{m} \right\rceil - \left\lfloor \frac{k}{m} \right\rfloor \right) = \begin{cases} 1 & \text{se } k \text{ é primo} \\ 0 & \text{caso contrário} \end{cases}$$

Em 1845 o matemático francês Bertrand conjecturou que para todo inteiro $n > 3$, existe algum primo p tal que $n < p < 2n - 2$. Esta afirmação ficou conhecida como

postulado de Bertrand, apesar de não ser um postulado, mas sim um teorema demonstrado por Chebyshev em 1852. Uma proposição mais fraca, porém esteticamente mais interessante, e que as vezes também é chamada de postulado de Bertrand, nos afirma que para todo inteiro n>1, existe algum primo no intervalo $(n,2n)$. Por maior motivo sempre existe algum número primo no intervalo $(n,2n]$, qualquer que seja o inteiro positivo n. Seja p o menor primo no intervalo $(n,2n]$. Então p é o menor primo maior que n. Mostrarei que $f(n) = p$. Primeiro note:

$$\frac{1}{2^p}=\frac{1}{2^p}g(p,n)\leq\sum_{k=n+1}^{2n}\frac{1}{2^k}g(k,n)=\text{parcelas}\ldots+\frac{1}{2^p}g(p,n)+\ldots\text{parcelas}$$

por outro lado, pela minimalidade de p tem-se:

$$\sum_{k=n+1}^{2n}\frac{1}{2^k}\underbrace{g(k,n)}_{\substack{=0\text{ se k não}\\ \text{é primo}}}=\sum_{k=p}^{2n}\frac{1}{2^k}g(k,n)<\sum_{k=p}^{\infty}\frac{1}{2^k}=\frac{2}{2^p}$$

logo

$$\frac{1}{2^p}\leq\sum_{k=n+1}^{2n}\frac{1}{2^k}g(k,n)<\frac{2}{2^p}$$

tomando o logaritmo na base 2 ter-se-á

$$-p\leq\log_2\sum_{k=n+1}^{2n}\frac{1}{2^k}\underbrace{\prod_{m=2}^{n}\left(\left\lceil\frac{k}{m}\right\rceil-\left\lfloor\frac{k}{m}\right\rfloor\right)}_{g(k,n)}<1-p$$

assim

$$-p=\left\lfloor\log_2\sum_{k=n+1}^{2n}\frac{1}{2^k}\prod_{m=2}^{n}\left(\left\lceil\frac{k}{m}\right\rceil-\left\lfloor\frac{k}{m}\right\rfloor\right)\right\rfloor$$

donde

$$f(n)=-\left\lfloor\log_2\sum_{k=n+1}^{2n}\frac{1}{2^k}\prod_{m=2}^{n}\left(\left\lceil\frac{k}{m}\right\rceil-\left\lfloor\frac{k}{m}\right\rfloor\right)\right\rfloor=p$$

Portanto $f(n) = p$ é o menor primo maior que n. De forma equivalente, aproveitando que $-\lfloor \log_2 x \rfloor = \lceil -\log_2 x \rceil = \lceil \log_{1/2} x \rceil$, tem-se também

$$f(n) = \left\lceil \log_{1/2} \sum_{k=n+1}^{2n} \frac{1}{2^k} \prod_{m=2}^{n} \left(\left\lceil \frac{k}{m} \right\rceil - \left\lfloor \frac{k}{m} \right\rfloor \right) \right\rceil = p$$

Fórmula 2. *Seja g a função dada por*

$$g(n) = \left\lfloor \log_2 \sum_{k=n+1}^{2n} 2^k \prod_{m=2}^{n} \left(\left\lceil \frac{k}{m} \right\rceil - \left\lfloor \frac{k}{m} \right\rfloor \right) \right\rfloor$$

então $g(n)$ é o maior primo menor ou igual a $2n$.

A prova da fórmula 2 é inteiramente similar à da fórmula 1.

5

Outras Fórmulas Relacionadas que Produzem Números Primos

A função de μ Mobius

Ela é definida por

$$\mu(1) = 1$$

e

$$\mu(n) = \begin{cases} 0 & \text{se existe } p \text{ primo tal que } p^2 \text{ divide } n \\ (-1)^k & \text{caso } n \text{ seja o produto de } k \text{ primos distintos} \end{cases}$$

Fórmula 1. Seja n um inteiro positivo qualquer e $n^\#$ o produto de todos os números primos no intervalo [1,n]. Então o menor primo maior que n é dado por

$$f(n) = \left\lceil \log_{1/2} \sum_{j=n+1}^{2n} \frac{1}{2^j} \left| \mu\left(jn^\# \right) \right| \right\rceil$$

ou, o que é o mesmo,

$$f(n) = -\left\lfloor \log_2 \sum_{j=n+1}^{2n} \frac{1}{2^j} \left| \mu\left(jn^\# \right) \right| \right\rfloor$$

Prova. Para $n = 1$ tem-se

$$f(1) = \left\lceil \log_{1/2} \sum_{j=1+1}^{2\times 1} \frac{1}{2^j} \left| \mu\left(j1^\# \right) \right| \right\rceil = \left\lceil \log_{1/2} \frac{1}{2^2} \left| \mu(2) \right| \right\rceil = \left\lceil \log_{1/2} \frac{1}{2^2} \right\rceil = 2$$

Isto confirma a fórmula neste caso. Note que $1^\# = 1$, pois $1^\# = \Pi_{x \in \varnothing} x$ é *produto vazio* que, como se sabe, é igual a 1.

Suponha $n > 1$ e seja p o menor primo maior que n. Seja ainda

$$S = \sum_{j=n+1}^{2n} \frac{1}{2^j} \left| \mu\left(jn^{\#} \right) \right|$$

O *postulado de Bertrand* afirma que existe pelo menos um primo no intervalo $(n, 2n-2)$, para todo inteiro $n > 3$. Esta afirmação é verdadeira de fato e nos garante que $p < 2n$. Pela minimalidade de p, se $n < j < p$ então j é composto. Como $j < p$ e $p < 2n$ então $j < 2n$ donde j, sendo composto, tem um fator primo q no intervalo $[2, n]$. Então $q \mid j$ e $q \mid n^{\#}$ e daí $q^2 \mid jn^{\#}$, donde $\mu\left(jn^{\#} \right) = 0$ para todo inteiro $j \in (n, p)$. Assim

$$\frac{1}{2^p} < S = \sum_{j=n+1}^{2n} \frac{1}{2^j} \left| \mu\left(jn^{\#} \right) \right| = \underbrace{0 + \ldots + 0}_{\substack{n<j<p \\ \mu\left(jn^{\#} \right)=0}} + \frac{1}{2^p} + \begin{pmatrix} \text{alguns inversos de} \\ \text{potências de 2} \end{pmatrix} < \frac{2}{2^p}$$

$$\therefore \frac{1}{2^p} < S < \frac{1}{2^{p-1}}$$

aplicando o logaritmo na base ½ tem-se

$$p - 1 < \log_{1/2} S < p$$

logo

$$\left\lceil \log_{1/2} S \right\rceil = p$$

isto é

$$f(n) = \left\lceil \log_{1/2} \sum_{j=n+1}^{2n} \frac{1}{2^j} \left| \mu\left(jn^{\#} \right) \right| \right\rceil$$

Como queríamos demonstrar.

Fórmula 2. Seja n um inteiro positivo qualquer e $n^{\#}$ o produto de todos os números primos no intervalo [1,n]. Então o maior primo menor ou igual a $2n$ é dado por

$$g(n) = \left\lfloor \log_2 \sum_{j=n+1}^{2n} 2^j \left|\mu\left(jn^{\#}\right)\right| \right\rfloor$$

A prova da fórmula 2 é inteiramente análoga à da fórmula 1.

6

Uma Aplicação da Análise à Teoria dos Números

Introdução.

Neste trabalho pressuponho que o leitor esteja familiarizado com certos conceitos da Análise, como sucessões, séries e convergência. Alguns teoremas da Análise Real são enunciados à medida que se tornam necessários para a compreensão do texto. Usando definições e teoremas da Análise, caracterizarei os números primos. Com essa caracterização construirei uma função que, dado n, fornece o valor de $\pi(n)$, isto é, a quantidade de números primos menores ou iguais a n. Também construirei uma função cuja imagem é o conjunto dos números primos. Ora, esses resultados são de interesse da Teoria dos Números. Eles são estudados aqui utilizando-se teoremas e definições da Análise Real. Portanto, este artigo é um exemplo de como dois ramos distintos da Matemática podem relacionar-se.

Seqüências duplas

A seguinte definição será muito importante para o desenvolvimento deste trabalho.

Definição 1. De acordo com LIMA (1976, p. 304) "Uma *seqüência dupla* (x_{nk}) é uma função $x:\mathbb{N}\times\mathbb{N}\to\mathbb{R}$ que associa a cada par (n, k) de números naturais um número real x_{nk}."

Podemos imaginar os números x_{nk} dispostos numa tabela que se estende infinitamente para a direita e para baixo. Assim, os índices n e k em x_{nk} indicam que esse número real ocupa a n-ésima linha e a k-ésima coluna da tabela.

Observação

Considere a seqüência dupla (x_{nk}) definida por

$$x_{nk} = \begin{cases} 1 - 1/2^n & \text{se } n = k \\ -1 + 1/2^n & \text{se } n + 1 = k \\ 0 & \text{nos outros casos} \end{cases}$$

A representação em tabela de (x_{nk}) é a seguinte:

$$\begin{array}{cccccccc}
\frac{1}{2} & -\frac{1}{2} & 0 & 0 & 0 & 0 & \cdots & \to 0 \\
0 & \frac{3}{4} & -\frac{3}{4} & 0 & 0 & 0 & \cdots & \to 0 \\
0 & 0 & \frac{7}{8} & -\frac{7}{8} & 0 & 0 & \cdots & \to 0 \\
0 & 0 & 0 & \frac{15}{16} & -\frac{15}{16} & 0 & \cdots & \to 0 \\
0 & 0 & 0 & 0 & \frac{31}{32} & -\frac{31}{32} & \cdots & \to 0 \\
0 & 0 & 0 & 0 & 0 & \frac{63}{64} & \cdots & \to 0 \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \quad \vdots \\
\downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \cdots & \\
\frac{1}{2} & \frac{1}{4} & \frac{1}{8} & \frac{1}{16} & \frac{1}{32} & \frac{1}{64} & \cdots &
\end{array}$$

A soma de cada linha é 0 logo $\Sigma_n\left(\Sigma_k x_{nk}\right) = \Sigma_n 0 = 0$. Por outro lado, a soma dos elementos da k-ésima coluna é $1/2^k$, logo $\Sigma_k\left(\Sigma_n x_{nk}\right) = \Sigma_k 1/2^k = 1$. Assim, dada uma seqüência dupla (x_{nk}), mesmo que as séries $\Sigma_n\left(\Sigma_k x_{nk}\right)$ e $\Sigma_k\left(\Sigma_n x_{nk}\right)$ convirjam, não é necessariamente verdadeiro que $\Sigma_n\left(\Sigma_k x_{nk}\right) = \Sigma_k\left(\Sigma_n x_{nk}\right)$.

Uma certa seqüência dupla

Examinemos a seqüência dupla (y_{nk}) definida por:

$$y_{nk} = \begin{cases} x^k & \text{se } n \text{ divide } k \text{ e } n \neq 1 \\ 0 & \text{caso contrário} \end{cases}$$

Representarei alguns termos dessa seqüência dupla na tabela que se segue:

	k	1	2	3	4	5	6	7	8	9	...
n											
1		0	0	0	0	0	0	0	0	0	...
2		0	x^2	0	x^4	0	x^6	0	x^8	0	...
3		0	0	x^3	0	0	x^6	0	0	x^9	...
4		0	0	0	x^4	0	0	0	x^8	0	...
5		0	0	0	0	x^5	0	0	0	0	...
6		0	0	0	0	0	x^6	0	0	0	...
7		0	0	0	0	0	0	x^7	0	0	...
8		0	0	0	0	0	0	0	x^8	0	...
9		0	0	0	0	0	0	0	0	x^9	...
...		...	...	...	...	...	...	...	...	...	...

A primeira linha (n = 1) é só de zeros, logo $\sum_k y_{1k} = 0$. É fácil ver que para a n-ésima linha, com n > 1, vale:

$$\sum_k y_{nk} = x^n + x^{2n} + x^{3n} + x^{4n} + \ldots = \frac{x^n}{1-x^n}$$

sempre que $x \in (-1,1)$. Definirei a função $L:(-1,1) \to \mathbb{R}$ como a soma dos termos da seqüência dupla (y_{nk}) linha por linha, isto é:

$$L(x) = \sum_n \left(\sum_k y_{nk} \right) = \sum_{n=2}^{\infty} \frac{x^n}{1-x^n}$$

precisamos verificar se a função L está bem definida, ou seja, se a série do lado direito da igualdade converge. Mas antes lembro uma definição: uma série $\sum a_n$ é *absolutamente convergente* quando a série formada pelo valor absoluto de seus termos converge, isto é, a série $\sum a_n$ é absolutamente convergente quando $\sum |a_n|$ converge. Lembro também que toda série que converge absolutamente é convergente.

Proposição 1: *Se* $\lim_{n\to\infty} \sqrt[n]{|a_n|} < 1$ *então a série* $\sum a_n$ *converge (absolutamente).*

Podemos agora mostrar que a série

$$L(x) = 0 + \frac{x^2}{1-x^2} + \frac{x^3}{1-x^3} + \frac{x^4}{1-x^4} + \cdots$$

converge (absolutamente). De fato

$$\lim_{n\to\infty} \sqrt[n]{\left|\frac{x^n}{1-x^n}\right|} = \frac{|x|}{\lim\limits_{n\to\infty} \sqrt[n]{1-x^n}} = |x| < 1$$

portanto a função $L:(-1,1) \to \mathbb{R}$ está bem definida.

Definirei agora a função $C:(-1,1) \to \mathbb{R}$ como a soma dos termos da seqüência dupla (y_{nk}) coluna por coluna, isto é, $C(x) = \sum_k \left(\sum_n y_{nk}\right)$. Pela observação feita neste artigo, não é evidente que $C(x) = L(x)$. É aí que entra a

Proposição 2. Conforme LIMA (1976, p. 305), "*Dada a seqüência dupla* (x_{nk})*, suponhamos que cada linha determine uma série absolutamente convergente, isto é,* $\sum_k |x_{nk}| = a_n$ *para cada n. Admitamos ainda que* $\sum_n a_n < +\infty$*. Então* $\sum_n \left(\sum_k x_{nk}\right) = \sum_k \left(\sum_n x_{nk}\right)$*.*"

Utilizando a proposição 2, vamos provar que $C(x) = L(x)$. A primeira linha da seqüência dupla (y_{nk}) é só de zeros, logo a série determinada por ela converge absolutamente (para zero). Para todo $x \in (-1,1)$ e para cada n = 2, 3, 4, ... é fácil ver que

$$\sum_k |y_{nk}| = |x^n| + |x^{2n}| + |x^{3n}| + |x^{4n}| + \cdots = \frac{|x^n|}{1-|x^n|}$$

portanto, toda linha da seqüência dupla (y_{nk}) determina uma série absolutamente convergente sempre que $|x| < 1$. Para que as condições da proposição 2 sejam satisfeitas, resta mostrar que $\sum_n \sum_k |y_{nk}| < +\infty$. De fato:

$$\sum_n \sum_k |y_{nk}| = \sum_{n=2}^{\infty}\left(|x^n| + |x^{2n}| + |x^{3n}| + |x^{4n}| + \cdots\right) = \sum_{n=2}^{\infty}\frac{|x^n|}{1-|x^n|} = L(|x|) < +\infty$$

$$\therefore \sum_n \sum_k |y_{nk}| < +\infty$$

Assim, de acordo com a proposição 2, podemos afirmar que $C(x) = L(x)$. Por outro lado não é difícil ver que $C(x) = \sum_k \sum_n y_{nk} = \Sigma_{k=1}^{\infty}\left(\mathrm{d}(k)-1\right)x^k$, onde $\mathrm{d}(k)$ é o número de divisores positivos de k. Como $C(x) = L(x)$, a expansão em série de Taylor de $L(x)$ em torno de $x = 0$ é $\Sigma_{k=1}^{\infty}\left(\mathrm{d}(k)-1\right)x^k$. Assim, pela unicidade da série de Taylor, se a sucessão (c_n) satisfaz

$$L(x) = \sum_{n=2}^{\infty}\frac{x^n}{1-x^n} = c_0 + c_1 x + c_2 x^2 + c_3 x^3 + \ldots + c_k x^k + \cdots$$

para todo $x \in (-1,1)$, então $c_0 = 0$ e $c_k = \mathrm{d}(k) - 1$ para $k > 0$.

Lema. *Se a função* $g:(-1,1) \to \mathbb{R}$ *é consistentemente definida por* $g(x) = \sum a_n x^n$, *então para cada número natural n a n-ésima derivada de g é obtida pela sucessiva derivação termo a termo da série* $\sum a_n x^n$.

É fácil ver que $L(0) = c_0$. Aplicando o lema acima, podemos derivar L sucessivamente e obter $L'(0) = c_1$, $L''(0) = 2c_2$, $L'''(0) = 6c_3$, $L^{(4)}(0) = 24c_4$, ..., $L^{(k)}(0) = k!c_k$, ..., portanto

$$L(x) = L(0) + L'(0)x + \frac{1}{2!}L''(0)x^2 + \frac{1}{3!}L'''(0)x^3 + \cdots + \frac{1}{k!}L^{(k)}(0)x^k + \cdots$$

Assim, os valores de c_1, c_2, c_3, ... ficam determinados a partir dos valores das derivadas sucessivas da função L no ponto 0. Especificamente tem-se que $c_k = L^{(k)}(0)/k!$.

Caracterizando números primos

Sabemos que um número natural k é primo se e só se d(k) = 2; sabemos também que $c_k = d(k) - 1$ e que $c_k = L^{(k)}(0) / k!$. Logo, um inteiro positivo k é primo se e somente se $c_k = 1$, isto é, se $L^{(k)}(0) = k!$. Se k for composto então $c_k > 1$ e $L^{(k)}(0) > k!$. Portanto, sendo $\lfloor u \rfloor$ o único número inteiro satisfazendo $\lfloor u \rfloor \leq u < \lfloor u \rfloor + 1$, vale:

$$\pi(n) = \sum_{k=2}^{n} \left\lfloor \frac{1}{c_k} \right\rfloor = \sum_{k=2}^{n} \left\lfloor \frac{k!}{L^{(k)}(0)} \right\rfloor$$

onde $\pi(n)$ é o número de primos p tais que $2 \leq p \leq n$. Além disso o conjunto dos números primos é a imagem da função f definida para os inteiros maiores que 1 e dada por

$$f(n) = 2 + (n-2) \left\lfloor \frac{1}{c_n} \right\rfloor = 2 + (n-2) \left\lfloor \frac{n!}{L^{(n)}(0)} \right\rfloor$$

7

Relacionando Números Primos e Binomiais

Introdução

Neste artigo o estudo da função $g(n) = \text{mdc}(C_{n,1}, C_{n,2}, \dots C_{n,n-1})$ nos conduzirá à uma fórmula que produz todos os números primos e apenas primos. Provar-se-á que $g(n) = 1$ se *n* tiver pelo menos dois fatores primos distintos e $g(n) = p$ se $n = p^m$ para algum primo *p* e algum inteiro positivo *m*. Portanto, o conjunto dos números primos é igual à imagem da função $f(n) = \max(2, g(n))$. Aproveitando que $C_{n,r} = C_{n,n-r}$ mostra-se que o conjunto dos primos coincide, também, com a imagem da função $f(n) = \max\left(2, \text{mdc}\left(\binom{2n+1}{1}, \binom{2n+1}{2}, \dots \binom{2n+1}{n}\right)\right)$

A função Λ Von Mangoldt é importante em Teoria dos Números. Ela é definida por

$$\Lambda(n) = \begin{cases} \log p, \text{ se } n \text{ é potência do primo } p \\ 0, \text{ caso contrário} \end{cases}$$

Uma conseqüência imediata do teorema demonstrado no presente trabalho é que $\Lambda(n) = \log g(n)$.

Uma função útil

Todo número racional pode ser escrito como produto de potências de números primos com expoentes inteiros. Assim, $21/160 = 2^{-5}3^{1}5^{-1}7^{1}11^{0}13^{0}17^{0}\cdots$ e $77/9 = 2^{0}3^{-2}5^{0}7^{1}11^{1}13^{0}17^{0}19^{0}\cdots$ As provas das proposições 1 e 2 que se seguem serão

facilitadas pelo uso da funções $\nu_p : \mathbb{Q} \to \mathbb{Z}$. O inteiro $\nu_p(b)$ é o expoente do primo p na representação do racional b como produto de potências de números primos. O leitor deve se convencer de que, fixado um primo p qualquer, a função ν_p satisfaz as seguintes propriedades para todos os racionais $x, y, z, ..., w$, todos os inteiros $a, b, c, ..., n$.

(i) $\nu_p(xyz\cdots w) = \nu_p(x) + \nu_p(y) + \nu_p(z) + \ldots + \nu_p(w)$

(ii) $\nu_p(p^n) = n$

(iii) $\nu_p(n) = 0$ se e só se p não divide n

(iv) $\nu_p(x/y) = \nu_p(x) - \nu_p(y)$

(v) $\nu_p(\text{mdc}(a,b,c,\ldots,n)) = \min(\nu_p(a), \nu_p(b), \nu_p(c), \ldots \nu_p(n))$

(vi) Se $\nu_p(a) \neq \nu_p(b)$ então $\nu_p(a \pm b) = \min(\nu_p(a), \nu_p(b))$

(vii) $\nu_p(-a) = \nu_p(a)$

(viii) $\nu_p(a) \geq 0$

(ix) Se $1 \leq a < p^n$ então $\nu_p(a) < n$

(x) $\nu_p(a!) = \sum_{t>0} \lfloor a/p^t \rfloor$

onde nesta última igualdade $\lfloor x \rfloor$ é o maior inteiro menor ou igual a x.

No que se segue usar-se-á $g(n) = \text{mdc}(C_{n,1}, C_{n,2}, \ldots C_{n,n-1})$.

Três lemas

Lema 1. *Seja n um inteiro positivo. Se n tem pelo menos dois fatores primos distintos então* $g(n) = 1$.

Prova. Como $g(n)$ divide $n = C_{n,1}$, todo fator primo de $g(n)$ é também fator de n. Para provar que $g(n) = 1$ basta mostrar que $g(n)$ não é divisível por nenhum fator

primo de n. Farei isso tomando um fator primo p genérico de n e mostrando que $\nu_p\left(g\left(n\right)\right)=0$. Suponhamos que $\nu_p\left(n\right)=v$:

$$0\le\nu_p\left(g\left(n\right)\right)=\min\left(\nu_p\left(C_{n,1}\right),\nu_p\left(C_{n,2}\right),\ldots,\nu_p\left(C_{n,n-1}\right)\right)\le$$

$$\le\nu_p\binom{n}{p^v}=\nu_p\left(\prod_{u=0}^{p^v-1}\frac{n-u}{p^v-u}\right)=\sum_{u=0}^{p^v-1}\nu_p\left(\frac{n-u}{p^v-u}\right)=$$

$$=\sum_{u=0}^{p^v-1}\left(\nu_p\left(n-u\right)-\nu_p\left(p^v-u\right)\right)=$$

$$=\left(\nu_p\left(n\right)-\nu_p\left(p^v\right)\right)+\sum_{u=1}^{p^v-1}\left(\nu_p\left(n-u\right)-\nu_p\left(p^v-u\right)\right)=$$

$$=\left(v-v\right)+\sum_{u=1}^{p^v-1}\left(\min\left(\nu_p\left(n\right),\nu_p\left(u\right)\right)-\min\left(\nu_p\left(p^v\right),\nu_p\left(u\right)\right)\right)=$$

$$=\sum_{u=1}^{p^v-1}\left(\nu_p\left(u\right)-\nu_p\left(u\right)\right)=\sum_{u=1}^{p^v-1}0=0$$

$\therefore 0\le\nu_p\left(g\left(n\right)\right)\le 0$

$\therefore \nu_p\left(g\left(n\right)\right)=0$ para cada fator primo p de n. Logo $g(n) = 1$.

Lema 2. *Suponha que $n = p^v$, p primo e v inteiro positivo. Então p divide $g(n)$.*

Prova. Como $C_{n,1}=n=p^v$ então $g(n)=p^s$ com s inteiro e $0\le s\le v$. Seja $r\in$ {1, 2, 3, ..., n – 1}, $r = kp^t$ onde p não divide $k\in\mathbb{N}$ e $t < v$.

$$\nu_p\binom{p^v}{r} = \nu_p\left(\frac{p^v!}{(p^v-r)!r!}\right) =$$

$$= \nu_p(p^v!) - \left(\nu_p\left((p^v-r)!\right) + \nu_p(r!)\right) =$$

$$= \sum_{t=1}^{v}\left\lfloor \frac{p^v}{p^t} \right\rfloor - \left(\sum_{t=1}^{v}\left\lfloor \frac{p^v-r}{p^t} \right\rfloor + \sum_{t=1}^{v}\left\lfloor \frac{r}{p^t} \right\rfloor\right) >$$

$$> \sum_{t=1}^{v}\frac{p^v}{p^t} - \left(\sum_{t=1}^{v}\frac{p^v-r}{p^t} + \sum_{t=1}^{v}\frac{r}{p^t}\right) =$$

$$= \sum_{t=1}^{v}\frac{p^v}{p^t} - \sum_{t=1}^{v}\frac{p^v}{p^t} = 0$$

Ficou provado que para cada $r = 1, 2, 3, ..., n - 1$ vale $\nu_p(C_{n,r}) \geq 1$, isto é, p divide $C_{n,r}$. Portanto p divide $g(n)$.

Lema 3. *Suponha que $n = p^v$, p primo e v inteiro positivo. Então p^2 não divide $g(n)$.*

Prova.

$$\nu_p(g(n)) = \min\left(\nu_p(C_{n,1}), \nu_p(C_{n,2}), \ldots, \nu_p(C_{n,n-1})\right) \leq$$

$$\leq \nu_p\binom{n}{p^{v-1}} = \nu_p\left(\prod_{u=0}^{p^{v-1}-1}\frac{p^v-u}{p^{v-1}-u}\right) = \sum_{u=0}^{p^{v-1}-1}\nu_p\left(\frac{p^v-u}{p^{v-1}-u}\right) =$$

$$= \sum_{u=0}^{p^{v-1}-1}\left(\nu_p(p^v-u) - \nu_p(p^{v-1}-u)\right) =$$

$$= \nu_p(p^v) - \nu_p(p^{v-1}) + \sum_{u=1}^{p^{v-1}-1}\left(\nu_p(p^v-u) - \nu_p(p^{v-1}-u)\right) =$$

$$= v - (v-1) + \sum_{u=1}^{p^{v-1}-1}\left(\min\left(\nu_p(p^v), \nu_p(u)\right) - \min\left(\nu_p(p^{v-1}), \nu_p(u)\right)\right) =$$

$$= 1 + \sum_{u=1}^{p^{v-1}-1}\left(\nu_p(u) - \nu_p(u)\right) = 1 + \sum_{u=1}^{p^{v-1}-1} 0 = 1 + 0 = 1$$

$\therefore \nu_p(g(n)) \leq 1$.

Logo p^2 não divide $g(n)$.

Observação 1. Dos lemas 2 e 3 concluímos que $g(n) = p$ sempre que n é potência do primo p.

Proposição. *Se n é um inteiro positivo, vale:*

$$\text{mdc}\left(\binom{n}{1},\binom{n}{2},\binom{n}{3},\ldots,\binom{n}{n-1}\right)=\begin{cases}p & \text{se } p \text{ é primo e } n = p^{v},\ v\in\mathbb{N}^{*}\\ 1 & \text{caso contrário}\end{cases}$$

A demonstração segue diretamente do lema 1 e da observação anterior.

Observação 2. Seja m o maior inteiro menor ou igual à metade de n. Desde que dois números binomiais complementares são iguais, isto é

$$\binom{x}{y}=\binom{x}{x-y}$$

tem-se

$$\text{mdc}\left(\binom{n}{1},\binom{n}{2},\binom{n}{3},\ldots\binom{n}{m}\right)=\text{mdc}\left(\binom{n}{1},\binom{n}{2},\binom{n}{3},\ldots,\binom{n}{n-1}\right)$$

Uma fórmula para os números primos

De acordo com a proposição e a observação 2, uma fórmula que produz todos os números primos e apenas primos é:

$$f(n)=\max\left(2, g(2n+1)\right)$$

isto é

$$f(n)=\max\left(2,\text{mdc}\left(\binom{2n+1}{1},\binom{2n+1}{2},\binom{2n+1}{3},\ldots,\binom{2n+1}{n}\right)\right)$$

onde a função f está definida no conjunto dos inteiros positivos e assumimos que mdc(a) = a para todo inteiro positivo a. É fácil ver que o conjunto dos números primos

é a imagem da função f dada acima. De fato, quando $2n+1$ admite dois ou mais fatores primos distintos, $f(n) = 2$; quando $2n+1$ é potência de um primo p, $f(n) = p$.

A função de Von Mangoldt

Ela é denotada é definida por:

$$\Lambda(n) = \begin{cases} \log p & \text{se } n = p^v \text{, para algum primo } p \text{ e algum inteiro } v \geq 1 \\ 0 & \text{caso contrário} \end{cases}$$

onde log é a função logaritmo natural. Conforme a proposição demonstrada, fica claro que:

$$\Lambda(n) = \log \operatorname{mdc}\left(\binom{n}{1}, \binom{n}{2}, \binom{n}{3}, \ldots, \binom{n}{n-1}\right)$$

A função de Von Mangoldt tem propriedades interessantes que as relacionam com outras funções importantes da Teoria dos Números, como a função zeta de Riemann e a função de Chebyshev.

8

Uma Função que Produz Infinitos Números Primos

Introdução

Mostrar-se-á no presente artigo que existe b real entre 5 e 5 + ¾, tal que todos os termos da sucessão $\lfloor b \rfloor, \lfloor b^b \rfloor, \lfloor b^{b^b} \rfloor, \ldots$ são números primos, onde $\lfloor x \rfloor$ é o maior inteiro menor ou igual a x.

Resultados similares foram obtidos por Mills em 1947 e por Wright em 1951. Mills mostrou que existe θ real tal que $\lfloor \theta^{3^n} \rfloor$ é um número primo para todo inteiro positivo n. Wright provou que existe um real ω tal que todos os números $\lfloor 2^{\omega} \rfloor, \lfloor 2^{2^{\omega}} \rfloor, \lfloor 2^{2^{2^{\omega}}} \rfloor, \ldots$ são primos.

A importância deste tipo de resultado está na demonstração da existência de certas constantes e não na obtenção de primos através de fórmulas. De fato, nem as funções de Mills e Wright, nem a função examinada neste artigo provam a primalidade de um número. Pelo contrário, para a determinação das respectivas constantes (θ, ω e b) com precisão suficiente para que qualquer dessas funções retorne um primo p, é necessário constatar a primalidade de p por outros processos.

A idéia básica da qual este trabalho se originou é a seguinte: escolhamos um primo x_1. É claro que $\lfloor x_1 \rfloor$ é primo. Agora escolhamos um real x_2 um pouquinho maior de modo que $\lfloor x_2 \rfloor = \lfloor x_1 \rfloor$ e $x_2^{x_2}$ sejam primos. Então $\lfloor x_2 \rfloor$ e $\lfloor x_2^{x_2} \rfloor$ são primos. Escolhamos um real x_3 ainda um pouco maior, mas de modo que $\lfloor x_3 \rfloor = \lfloor x_2 \rfloor = \lfloor x_1 \rfloor$, $\lfloor x_3^{x_3} \rfloor = \lfloor x_2^{x_2} \rfloor$ e $x_3^{x_3^{x_3}}$ sejam primos, e assim por diante. Se $b = \lim x_n$ então $\lfloor b \rfloor, \lfloor b^b \rfloor, \lfloor b^{b^b} \rfloor, \ldots$ são todos números primos. Os detalhes da demonstração e o resultado principal estão a seguir.

Uma função que produz infinitos primos

Definindo indutivamente $z*1=z;\ z*(m+1)=z^{z*m}$ e sendo $\lfloor z\rfloor$ o maior inteiro menor ou igual a z será demonstrada a existência de um real b tal que para todo inteiro positivo n, $\lfloor b*n\rfloor$ é um número primo. Se f é a função definida no conjunto dos inteiros positivos, dada por $f(n)=\lfloor b*n\rfloor$, ela produzirá infinitos números primos.

Lema 1. *Para todo inteiro positivo m e todos números reais u, v com u > v ≥ 3, vale*

$$\frac{u*(m+1)-v*(m+1)}{u*m-v*m}>3$$

Prova. Seja $g(x) = v^x$ com $x > 1$ e $v \geq 3$. Então $g'(c) = v^c \cdot ln(v) > 3$ sempre que $c > 1$.

$$\frac{v^a-v^b}{a-b}=\frac{g(a)-g(b)}{a-b}=g'(c)>3$$

Como g é contínua, pelo *Teorema do valor médio* tem-se que para todos $a,b>1$, vale: para algum $c\in(a,b)$. Tomando $a = u*m$ e $b = v*m$, tem-se que $a,b>1$ e

$$\frac{v^{u*m}-v^{v*m}}{u*m-v*m}>3$$

Como $u > v$, então

$$\frac{u^{u*m}-v^{v*m}}{u*m-v*m}>3$$

Isto é

$$\frac{u*(m+1)-v*(m+1)}{u*m-v*m}>3$$

Como queríamos provar.

Lema 2. *Dado um intervalo I* = [*r, s*], *se s/r* ≥ 2 e *s ≥ 1 então existe um número primo em I.*

Prova. Se *s/r* ≥ 2 e *r* ≥ 1 então *I* contém um real maior ou igual a 1 e seu dobro. Porém, conforme o *postulado de Bertrand*, sempre existe um primo entre esses dois números, de modo que *I* sempre contém um número primo.

Lema 3. *Para todo inteiro positivo n e todo real v ≥ 5, existe u ≥ v satisfazendo:*

(i) $u*n - v*n \leq \frac{1}{2}$

(ii) $u*(n+1)$ *é primo*

Prova. Seja $v + \Delta$ o maior valor que podemos atribuir a u de modo que se cumpra a condição (i) acima, isto é, Δ satisfaz:

$$(v + \Delta)*n - v*n = ½$$

Então $u*(n + 1)$ pode assumir qualquer valor no intervalo $I = [v*(n + 1), (v + \Delta)*(n + 1)]$. Considere o quociente:

$$\mu = \frac{(v+\Delta)*(n+1)}{v*(n+1)}$$

Conforme o lema 2, se μ ≥ 2 então existirá algum primo no intervalo *I* e portanto poder-se-á escolher *u* satisfazendo (i) e (ii). Resta mostrar que μ ≥ 2. Tem-se:

$$(v+\Delta)*n - v*n = \frac{1}{2} \Leftrightarrow (v+\Delta)*n = (v*n) + \frac{1}{2} \Leftrightarrow (v+\Delta)^{(v+\Delta)*n} = (v+\Delta)^{(v*n)+1/2} \Leftrightarrow$$

$$\Leftrightarrow (v+\Delta)*(n+1) = (v+\Delta)^{(v*n)+1/2} \Leftrightarrow \frac{(v+\Delta)*(n+1)}{v*(n+1)} = \frac{(v+\Delta)^{(v*n)+1/2}}{v*(n+1)} \Leftrightarrow$$

$$\Leftrightarrow \mu = \frac{(v+\Delta)^{(v*n)+1/2}}{v^{v*n}} \Rightarrow \mu \geq \frac{v^{(v*n)+1/2}}{v^{v*n}} = v^{1/2} \Leftrightarrow \mu \geq \sqrt{v} \geq \sqrt{5} > 2$$

$$\therefore \mu \geq 2$$

e fica provado o lema 3.

Lema 4. *Seja* (x_n) *uma sucessão não decrescente de números não menores que* 3. *Se* $x_{n+1}*n - x_n*n \leq ½$, *então* $x_{n+1}*j - x_n*j \leq 2^{-1}3^{j-n}$, *para* $j = 1, 2, 3, ..., n$.

Prova. O caso $x_n = x_{n+1}$ é trivial. Suponha que $0 < x_{n+1}*n - x_n*n \leq ½$. Fazendo, no lema 1, $u = x_{n+1}$ e $v = x_n$, tem-se

$$\frac{x_{n+1}*(m+1) - x_n*(m+1)}{x_{n+1}*m - x_n*m} > 3$$

Donde

$$\frac{x_{n+1}*n - x_n*n}{x_{n+1}*j - x_n*j} = \prod_{k=j}^{n-1} \frac{x_{n+1}*(k+1) - x_n*(k+1)}{x_{n+1}*k - x_n*k} > \prod_{k=j}^{n-1} 3 = 3^{n-j}$$

Para $j = 1, 2, 3, ..., n - 1$. Logo:

$$\frac{x_{n+1}*n - x_n*n}{x_{n+1}*j - x_n*j} > 3^{n-j} \Rightarrow \frac{x_{n+1}*j - x_n*j}{x_{n+1}*n - x_n*n} < 3^{j-n} \Rightarrow x_{n+1}*j - x_n*j < \frac{3^{j-n}}{2}$$

Como queríamos.

Lema 5. *Seja* (x_n) *uma sucessão não decrescente de números não menores que* 3. *Se* $x_{n+1}*n - x_n*n \leq ½$, *então para todos inteiros positivos j, n com* $j \leq n$ *vale* $x_j*j \leq x_n*j < ¾ + x_j*j$.

Prova. O caso $j = n$ é trivial. Suponha $j < n$. Conforme o lema 4 tem-se as seguintes desigualdades:

$0 \leq x_{j+1}*j - x_j*j \leq 2^{-1}3^0$

$0 \leq x_{j+2}*j - x_{j+1}*j \leq 2^{-1}3^{-1}$

$0 \leq x_{j+3}*j - x_{j+2}*j \leq 2^{-1}3^{-2}$

....

$0 \leq x_n*j - x_{n-1}*j \leq 2^{-1}3^{j-n+1}$

Somando estas desigualdades tem-se:

$$0 \leq x_n*j - x_j*j \leq 2^{-1}3^0 + 2^{-1}3^{-1} + 2^{-1}3^{-2} + ... + 2^{-1}3^{j-n+1} < ¾$$

isto é $0 \leq x_n*j - x_j*j < ¾$, ou seja $x_j*j \leq x_n*j \leq ¾ + x_j*j$. Fica assim provado o lema 5.

Proposição. *Seja* (x_n) *uma sucessão não decrescente com* $x_1 = 5$ *satisfazendo, para todo inteiro positivo n, as duas condições seguintes:*

(i) $x_{n+1}*n - x_n*n \leq ½$

(ii) $x_{n+1}*(n + 1)$ *é primo*

Se $b = \lim x_n$ *então* $\lfloor b*n \rfloor$ *é um número primo para todo inteiro positivo n.*

Prova. O lema 3 garante a existência da sucessão (x_n). De fato, como $x_1 = 5$, o lema 3 garante a existência de x_2 satisfazendo $x_2*1 - x_1*1 \leq ½$ e x_2*2 primo. Assim, dado x_1, construímos x_2 satisfazendo (i) e (ii) (para $n = 1$) . Supondo que já construímos $x_1, x_2, ..., x_n$, o lema 3 garante a existência de x_{n+1} satisfazendo (i) e (ii). Portanto existe uma sucessão (x_n) satisfazendo (i) e (ii) para todo inteiro positivo n.

Afirmo que (x_n) tem limite. Com efeito, conforme o lema 5, para todo $j \leq n$, vale $x_j*j \leq x_n*j < ¾ + x_j*j$. Em particular, para $j = 1$ tem-se $5 = x_1 = x_1*1 \leq x_n = x_n*1 < ¾ + x_1*1 = ¾ + 5$ para todo n inteiro positivo, isto é, $x_n \leq 5 + ¾$. Como x_n é uma sucessão não decrescente limitada superiormente (por $5 + ¾$) então existe $b = \lim x_n$.

Conforme o lema 5, para todos inteiros n, j com $j \leq n$, vale $x_j*j \leq x_n*j \leq ¾ + x_j*j$. Fazendo n tender a infinito tem-se $x_j*j \leq b*j \leq ¾ + x_j*j$ para todo inteiro positivo j.

Porém x_j*j é primo por hipótese, donde $\lfloor b * j \rfloor = x_j * j$ é primo para todo inteiro positivo j.

Com isso fica provado que existe um número real b, entre 5 e 5+3/4, tal que a sucessão $\lfloor b \rfloor, \lfloor b^b \rfloor, \lfloor b^{b^b} \rfloor, \ldots$ é formada apenas por números primos. Então uma função que produz infinitos números primos, e apenas primos, é dada por:

$$f(n) = \underbrace{\left\lfloor b^{b^{\cdot^{\cdot^{b}}}} \right\rfloor}_{n \text{ bês}}$$

Perspectivas

A prova da proposição acima pode ser modificada para demonstrar a existência de outras funções que produzem infinitos números primos. Portanto, o resultado obtido pode ser estendido para todo um conjunto de funções que satisfizerem determinados critérios. Isto significa que outros problemas semelhantes podem ser resolvidos através da técnica utilizada neste trabalho.

9

Uma Função para o enésimo Número Primo

Introdução

Será apresentada uma função f definida recursivamente tal que $\lfloor f(n) \rfloor = p_n$, onde $\lfloor x \rfloor$ é o maior inteiro menor ou igual a x e p_n é o n-ésimo número primo.

Frações contínuas

Uma fração contínua *finita* em n variáveis a_1, a_2, a_3, ..., a_n é denotada e definida por:

$$[a_1, a_2, a_3, \ldots, a_n] = a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \ddots \cfrac{}{\cfrac{1}{a_n}}}}$$

Se os números a_2, a_3, ..., a_n são inteiros positivos, a fração contínua acima é dita simples.

Observação

O teorema 165 de [8] garante que para toda sucessão (a_n) de inteiros positivos existe o limite de $[a_1,a_2,a_3,...,a_n]$, quando n tende a infinito. Designamos esse limite por $[a_1,a_2,a_3,...]$, que é uma fração contínua simples *infinita*.

O teorema 168 da mesma referência garante que se $x=[a_1,a_2,a_3,...]$ é uma fração contínua simples infinita então $\lfloor x \rfloor = a_1$. Então, se escrevermos $\tilde{a}_n$ para denotar $[a_n,a_{n+1},a_{n+2},...]$ ter-se-á $\lfloor \tilde{a}_n \rfloor = a_n$.

Proposição. *Seja* (a_n) *uma sucessão de inteiros positivos. Definindo recursivamente*

$$\begin{cases} f(1) = [a_1, a_2, a_3, \ldots] \\ f(n+1) = \dfrac{1}{\{f(n)\}} \quad \text{para } n = 1, 2, 3, \ldots \end{cases}$$

onde $\{f(n)\}$ *é a parte fracionária de* $f(n)$*, definida por* $\{f(n)\} = f(n) - \lfloor f(n) \rfloor$*, tem-se que* $\lfloor f(n) \rfloor = a_n$.

Prova. Afirmo que $f(n) = \tilde{a}_n = [a_n,a_{n+1},...]$. A prova será por indução. Para $n = 1$ tem-se $f(1) = [a_1,a_2,a_3,...] = \tilde{a}_1$. Logo, a afirmação vale para $n = 1$.

Suponha que vale para $n = k$, isto é, suponha que $f(k) = \tilde{a}_k$. Mostrarei que $f(k+1) = \tilde{a}_{k+1}$.

$$f(k+1) = \frac{1}{\{f(k)\}} = \frac{1}{\{\tilde{a}_k\}} = \frac{1}{\{[a_k, a_{k+1}, \ldots]\}} = \frac{1}{\left\{a_k + \dfrac{1}{[a_{k+1}, a_{k+2}, \ldots]}\right\}}$$

$$= \frac{1}{\left\{a_k + \dfrac{1}{\tilde{a}_{k+1}}\right\}} = \frac{1}{1/\tilde{a}_{k+1}} = \tilde{a}_{k+1} \qquad \therefore f(k+1) = \tilde{a}_{k+1}$$

Logo, se a afirmação vale para $n=k$, também vale para $n=k+1$. Ficou provado que $f(n)=\tilde{a}_n$ para todo inteiro positivo n. Conforme a observação anterior, vale $\lfloor \tilde{a}_n \rfloor = a_n$. Portanto, para todo inteiro positivo n, $\lfloor f(n) \rfloor = a_n$.

Uma função para o *n*-ésimo número primo

Em particular, definindo recursivamente a função f por

$$\begin{cases} f(1) = [2, 3, 5, 7, 11, \ldots, p_n, \ldots] = 2{,}3130367364335829064\ldots \\ f(n+1) = \dfrac{1}{\{f(n)\}} \quad \text{para } n = 1, 2, 3, \ldots \end{cases}$$

Vale $\lfloor f(n) \rfloor = p_n$.

10

Números Primos e Séries Formais

Introdução

Este trabalho aborda as séries formais, mostrando um modo de caracterizar números primos através delas. Também será apresentada uma fórmula para primos cuja base é essa caracterização.

Séries Formais

Uma série formal na indeterminada *x* é uma expressão que pode ser escrita como

$$p(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \dots$$

Todo polinômio pode ser interpretado como uma série formal. Por exemplo:

$$1 + 3x + 4x^2 = 1 + 3x + 4x^2 + 0x^3 + 0x^4 + \dots$$

A soma e o produto de séries formais decorrem de modo natural da soma e produto de polinômios. Somamos e multiplicamos séries formais como se estivéssemos trabalhando com polinômios. Assim, se $p(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \dots$ e $q(x) = b_0 + b_1 x + b_2 x^2 + b_3 x^3 + \dots$, então

$$p(x) + q(x) = (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + (a_3 + b_3)x^3 + \dots$$

$$p(x)q(x) = c_0 + c_1 x + c_2 x^2 + c_3 x^3 + \dots$$

onde

$$
\begin{aligned}
&c_0 = a_0 b_0 \\
&c_1 = a_1 b_0 + a_0 b_1 \\
&c_2 = a_2 b_0 + a_1 b_1 + a_0 b_2 \\
&c_3 = a_3 b_0 + a_2 b_1 + a_1 b_2 + a_0 b_3 \\
&\text{etc.}
\end{aligned}
$$

Séries formais podem ter mais de uma indeterminada:

$$Q(x, y) = \sum_{i,j=1}^{\infty} ijx^i y^j = xy + 2x^2 y + 2xy^2 + 3x^3 y + 3xy^3 + 4x^2 y^2 + \ldots$$

$$R(x, y, z) = \sum_{i=1}^{\infty} x^i y^{2i+1} z^{3i+2} = xy^3 z^5 + x^2 y^5 z^8 + x^3 y^7 z^{11} + \ldots$$

Além disso, observando que

$$
\begin{aligned}
&\left(1 + 2x + 4x^2 + 8x^3 + \ldots\right)(1 - 2x) = \\
&= 1 + 2x - 2x + 4x^2 - 4x^2 + 8x^3 - 8x^3 + \ldots = 1 \\
&\therefore \left(1 + 2x + 4x^2 + 8x^3 + \ldots\right)(1 - 2x) = 1
\end{aligned}
$$

e dividindo a última igualdade por $1 - 2x$ tem-se que

$$\frac{1}{1 - 2x} = 1 + 2x + 4x^2 + 8x^3 + \ldots$$

donde o quociente entre dois polinômios pode ser escrito como uma série formal.

Partições não ordenadas

Uma partição de um inteiro positivo n é a decomposição deste inteiro como soma de parcelas inteiras e positivas. Assim, 1+1+3 é uma partição do inteiro 5. Uma partição é não ordenada quando a ordem das parcelas é indiferente, isto é, 1+1+3, 1+3+1 e 3+1+1 representam a mesma partição não ordenada de 5. Note que a partição 1+1+3 tem três parcelas mas apenas dois termos distintos (1 e 3). Do mesmo modo a partição (de 14) 4+4+2+2+2 tem cinco parcelas, mas apenas duas parcelas distintas (4 e 2). A partição 2+2+2 (de 6) tem 3 parcelas, mas apenas um termo (somente o 2).

Número de partições não ordenadas

Denota-se por $[x^n]p(x)$ o coeficiente de x^n na série formal $p(x)$; por $[x^n y^m]p(x, y)$ o coeficiente de $x^n y^m$ na série formal $p(x, y)$ etc. Seja

$$\begin{aligned} p_j(x,y) &= 1 + x^j y + x^{j+j} y + x^{j+j+j} y + \ldots = \\ &= 1 + x^j y + x^{2j} y + x^{3j} y + \ldots = 1 + y\frac{x^j}{1-x^j} = \\ &= \frac{1 + x^j(y-1)}{1-x^j} \end{aligned}$$

Afirmo que o número de partições não ordenadas de n com exatamente k termos distintos é:

$$\left[x^n y^k\right] \prod_{j \geq 1} p_j(x,y)$$

Sejam $Q(x,y) = \prod_{j \geq 1} p_j(x,y)$ e

$$\begin{aligned} &a_1 + a_2 + \ldots + a_\alpha = n \\ &b_1 + b_2 + \ldots + b_\beta = n \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ &l_1 + l_2 + \ldots l_\gamma = n \end{aligned}$$

todas as partições de n com exatamente k termos distintos. Considere $A=[x^n y^k]Q(x, y)$ o coeficiente de $x^n y^k$ em $Q(x, y)$. Digamos que a partição de n com k termos distintos $c_1 + c_2 + \ldots + c_\delta = n$ tenha S_1 termos iguais a R_1; S_2 termos iguais a R_2; ... S_k termos iguais R_k. Então a partição $c_1 + c_2 + \ldots + c_\delta = n$ corresponde, pela propriedade distributiva, ao termo $x^n y^k$ obtido ao multiplicarmos

$$x^{R_1+R_1+\ldots+R_1}y = x^{S_1R_1}y \quad \text{(termo de } p_{R_1}(x,y)\text{)}$$
$$x^{R_2+R_2+\ldots+R_2}y = x^{S_2R_2}y \quad \text{(termo de } p_{R_2}(x,y)\text{)}$$
....
$$x^{R_k+R_k+\ldots+R_k}y = x^{S_kR_k}y \quad \text{(termo de } p_{R_k}(x,y)\text{)}$$
$$1=1 \quad \text{(termo de } p_T(x,y),\ T \neq R_1, R_2, \ldots R_k\text{)}$$

obtendo $x^{S_1R_1+S_2R_2+\ldots S_kR_k}y^k = x^{c_1+c_2+\ldots c_\delta}y^k = x^n y^k$

Portanto, ao desenvolver-se o produto $p_1(x,y)\,p_2(x,y)\,p_3(x,y)\ldots$ obtém-se, após aplicada a propriedade distributiva, tantos termos $x^n y^k$ quantas forem as partições não ordenadas de *n* com exatamente *k* termos distintos. Logo, o coeficiente de $x^n y^k$ em $Q(x,y)$ é o número de partições não ordenadas de *n* com exatamente *k* termos distintos.

Um caso especial

Quando $k=1$ as partições de *n* são somas de parcelas iguais. Por exemplo, para $n=6$ e $k=1$ temos as seguintes partições:

6 = 1+1+1+1+1+1

6 = 2+2+2

6 = 3+3

6 = 6

Logo $[x^6y]Q(x, y) = 4$ (4 partições de 6 como soma de parcelas iguais). De modo mais geral,

$$\left[x^n y\right]Q(x,y) = d(n)$$

onde $d(n)$ é o número de divisores de *n*. Daí, como

$$Q(x,y) = \prod_{j\geq 1}\left(1 + y\frac{x^j}{1-x^j}\right)$$

tem-se a seguinte

Proposição. *Se* $f(n) = \left[x^n y\right] \prod_{j \geq 1} \left(1 + y \frac{x^j}{1 - x^j}\right)$ *então f*(*n*) *é igual ao número de divisores positivos de n. Em particular n é primo se e só se f*(*n*)=2.

Desta proposição decorrem

Duas fórmulas

Será usada, aqui, a notação $\lfloor r \rfloor$ para designar o maior número real menor ou igual a *r*.

Se $Q(x, y) = \prod_{j \geq 1} \left(1 + y \frac{x^j}{1 - x^j}\right)$ e g é uma função definida no conjunto dos inteiros positivos e dada por $g(n) = 2 + (n-1)\left\lfloor \frac{2}{\left[x^{n+1} y\right] Q(x, y)} \right\rfloor$, então a imagem de g é o conjunto de todos os números primos. Além disso,

$$\pi(n) = -2 + \sum_{i=1}^{n} \left\lfloor \frac{2}{\left[x^i y\right] Q(x, y)} \right\rfloor$$

onde $\pi(n)$ é a quantidade de números primos no intervalo [1, *n*]

11

Caracterizando Intervalos de Números Primos através de Polinômios

Introdução

Sabemos que não existe nenhum polinômio não constante $P(x)$, com coeficientes inteiros, tal que $P(n)$ seja primo para todo inteiro positivo n (veja [13], ou a página 18 da referência [8]). Este resultado, embora negativo, mostra o interesse de se relacionar os números primos aos valores assumidos por um polinômio. Outro resultado neste sentido, porém muito mais surpreendente, diz que o conjunto dos números primos coincide com o dos valores positivos assumidos por um certo polinômio de grau 25, em 26 variáveis, quando estas percorrem o conjunto dos inteiros não negativos (veja capítulo 3.III da referência [4]). Os matemáticos têm-se interessado, portanto, em estabelecer relações entre números primos e polinômios. É neste contexto que se insere o presente trabalho.

Seja p_n o n-ésimo número primo. Provaremos nesta nota, um teorema que mostra como construir um polinômio P_n, de grau $p_n - 1$, que caracterizará todos os primos entre p_n e p_{n+1}^2. Se o inteiro m, satisfazendo $p_n < m < p_{n+1}^2$, satisfizer a condição adicional de que $p_1 p_2 \cdots p_n$ divide $P_n(m)$, então m será primo. Caso contrário, não o será.

Definições preliminares

Dois números inteiros são *congruentes módulo m* quando deixam o mesmo resto na divisão por m. Caso contrário são ditos *incongruentes módulo m*. Se a e b são congruentes módulo m, denotarei isso escrevendo $a \equiv b \mod m$. Caso contrário, se a e b forem incongruentes mod m, denotarei isto por $a \not\equiv b \mod m$. Note que tem-se $a \equiv b \mod m$ se e só se m divide $a - b$.

Chama-se *sistema completo de restos módulo m* (SCR mod *m*) todo conjunto $S \subset \mathbb{Z}$ com *m* elementos incongruentes módulo *m*. De outro modo: um *sistema completo de restos módulo m* é um conjunto de *m* números inteiros cujos restos na divisão por *m* são dois a dois diferentes. Tem-se que *S* é um SCR módulo *m* se, e só se, todo número inteiro é congruente módulo *m* a exatamente um elemento de *S*.

A função φ de Euler, definida para todo inteiro positivo *n*, retorna o número de inteiros positivos $\leq n$ que são relativamente primos com *n*. Isto é, $\varphi(n)$ é o número de elementos do conjunto $\{x \in \mathbb{N} : 1 \leq x \leq n \text{ e } \operatorname{mdc}(x,n) = 1\}$.

Um *sistema reduzido de restos módulo m* (SRR mod *m*) é um conjunto de $\varphi(m)$ inteiros incongruentes módulo *m*. Seja *S* um subconjunto qualquer de $\mathbb{Z}$. Então *S* é um SRR mod *m* se, e somente se, todo inteiro relativamente primo com *m* é congruente a exatamente um elemento de *S*.

Se *p* é primo então um exemplo de SRR mod *p* é $\{1, 2, 3, \ldots, p-1\}$.

O Resultado principal

Teorema 1. *Seja m um inteiro e* $P_n(x) = \prod_{i=1}^{p_n - 1}(x - a_i)$ *um polinômio com raízes inteiras satisfazendo*

(i) *Nenhum* a_i, $i = 1, 2, \ldots, p_n - 1$, *é divisível por nenhum primo* $p \leq p_n$.

(ii) *Para cada primo* $p \leq p_n$, o conjunto $\{a_1, a_2, \ldots a_{p_n - 1}\}$ *contém um sistema reduzido de restos módulo p*.

(iii) $p_n < m < p_{n+1}^2$.

Então o produto $p_1 p_2 \cdots p_n$ *divide* $P_n(m) = \prod_{i=1}^{p_n - 1}(m - a_i)$ *se, e somente se, m é um número primo.*

Prova. Denotaremos por $c^{\#}$ o produto $p_1 p_2 \cdots p_i$, sempre que $p_i \leq c < p_{i+1}$.

Suponha que $p_n^{\#}$ divide $P_n(m)$. Vamos provar que *m* é primo. Ora, se $m < p_{n+1}^2$ fosse composto, admitiria um fator primo menor ou igual a p_n. Basta, portanto, mostrar que nenhum primo $p \leq p_n$ divide *m*.

Seja p um primo tal que $p \leq p_n$. Como p é fator de $p_1 p_2 \cdots p_n = p_n^{\#}$ e $p_n^{\#} \mid P_n(m)$, então $p \mid (m-a_1)(m-a_2)\cdots(m-a_{p_n-1})$. Logo, para algum $i = 1, 2, \ldots, p_n - 1$ tem-se $p \mid m - a_i$. Se fosse $p \mid m$, teríamos $p \mid a_i$, o que contradiz (i). Assim, nenhum primo $p \leq p_n$ divide $m < p_{n+1}^2$ e portanto *m* é primo.

Suponha, agora, que $m > p_n$ é primo. Vamos provar que $p_n^{\#}$ divide $P_n(m)$. Para isto, provaremos que cada primo *p*, satisfazendo $p \leq p_n$ divide $P_n(m)$. Seja *p* um primo genérico tal que $p \leq p_n$. Como p e m são relativamente primos, e $\{a_1, a_2, \ldots a_{p_n-1}\}$ contém um SRR mod p conforme (ii), tem-se que existe a_i, $1 \leq i \leq p_n - 1$, tal que $m \equiv a_i \bmod p$. Daí $p \mid m - a_i$ e assim $p \mid P_n(m)$. Portanto, todo primo $p \leq p_n$ divide $P_n(m)$, isto é, $p_1 p_2 \cdots p_n$ divide $P_n(m)$ sempre que $m > p_n$ for primo.

A questão da existência

O leitor atento deve ter notado que o teorema faz afirmações envolvendo certos inteiros a_i's, mas nada afirma sobre a existência destes a_i's, muito menos mostra como calculá-los. Tudo o que dissemos até agora teria pouco valor se esta questão não fosse resolvida. Felizmente, esse não é um problema difícil. Seja p_n o *n*-ésimo número primo e tome $a_1 = 1$. Assim, nenhum dos primos $p_1, p_2, \ldots p_n$ divide a_1 e $\{a_1\}$ é um SRR mod 2. Agora, para cada inteiro i, $1 < i < p_n$, faça

$$c_i = \text{mmc}(p_1 p_2 \ldots p_n, i), \quad b_i = \frac{c_i}{i}, \quad a_i = i + b_i$$

Seja $p \leq p_n$ primo. Queremos provar que a condição (ii) do teorema se verifica. Para isto, é suficiente mostrar que $\{a_1, a_2, \ldots a_{p-1}\}$ é um SRR mod *p*. Com este propósito

mostraremos que $a_i \equiv i \bmod p$, sempre que $1 \le i < p$. Para $i=1$ já vimos que $a_i \equiv i \bmod p$. Para $i = 2,3,\ldots,p-1$ tem-se $p \mid c_i$ e $p \nmid i$ donde $p \mid \frac{c_i}{i}$, isto é, $p \mid b_i$. Como $a_i = i + b_i$, tem-se $a_i \equiv i \bmod p$ e, portanto, a condição (ii) do teorema é satisfeita.

Mostraremos, agora, que a condição (i) do teorema se verifica. Seja $p \le p_n$ um número primo. Se $p \mid i$, então a maior potência de *p* que divide *i* é a mesma que divide c_i e portanto $p \nmid b_i$. Logo, *p* não divide $a_i = i + b_i$, pois *p* divide *i* mas não divide b_i. Se $p \nmid i$ então, como $p \mid c_i$, tem-se que $p \mid b_i$. Portanto, *p* não divide $a_i = i + b_i$, pois *p* divide b_i mas não divide *i*. Em ambos os casos *p* não divide a_i. Então, nenhum dos primos $p_1, p_2, \ldots, p_n$ divide qualquer a_i. Isto é, a condição (i) do teorema também é verificada.

Exemplos

Fazendo $a_1=1$ e utilizando as fórmulas $c_i = \text{mmc}(p_1 p_2 \ldots p_n, i)$, $b_i = \frac{c_i}{i}$, $a_i = i + b_i$ para $1 < i < p_n$, tem-se

$P_2(x) = (x-1)(x-5) \equiv x^2 - 1 \bmod 3^\#$

Se $3 < x < 5^2$ então *x* é primo se e só se $3^\# = 6$ divide $P_2(x)$

$P_3(x) = (x-1)(x-17)(x-13)(x-19) \equiv x^4 + 10x^3 - 10x - 1 \bmod 5^\#$

Se $5 < x < 7^2$ então *x* é primo se e só se $5^\# = 30$ divide $P_3(x)$

$$P_4(x) = (x-1)(x-107)(x-73)(x-109)(x-47)(x-41) \equiv$$
$$\equiv x^6 + 42x^5 - 63x^4 - 21x^2 - 42x + 83 \bmod 7^\#$$

Se $7 < x < 11^2$ então *x* é primo se e só se $7^\# = 210$ divide $P_4(x)$

Teorema 2. Seja (b_{ij}) uma matriz tal que

(a) p_j não divide nenhum elemento da *j*-ésima coluna

(b) O conjunto dos termos da *j*-ésima coluna contem um SRR módulo p_j

Se para $i = 1, 2, 3, \ldots p_n - 1$ valer

$$[*]\begin{cases} a_i \equiv b_{i1} \mod p_1 \\ a_i \equiv b_{i2} \mod p_2 \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ a_i \equiv b_{in} \mod p_n \end{cases}$$

Então as condições (i) e (ii) do Teorema 1 são satisfeitas, isto é,

(i) *Nenhum* $a_i, i = 1, 2, \ldots, p_n - 1$, *é divisível por nenhum primo* $p \le p_n$.

(ii) *Para cada primo* $p \le p_n$, o conjunto $\{a_1, a_2, \ldots a_{p_n - 1}\}$ *contém um sistema reduzido de restos módulo p.*

Prova. Seja $p = p_j \le p_n$. Como $a_i \equiv b_{ij} \mod p$ (de [*]) e $p \nmid b_{ij}$ (de (a)) então $a_i \equiv b_{ij} \not\equiv 0 \mod p$ donde $a_i \not\equiv 0 \mod p$, isto é, $p \nmid a_{ij}$ para todo primo $p \le p_n$ e todo $i = 1, 2, 3, \ldots p_n - 1$. Logo a condição (i) do teorema 1 é satisfeita.

Seja $p = p_j \le p_n$. Conforme (b) existe um SRR $\mod p$ contido em $\{b_{ij}\}_{1 \le i < p_n}$. Aproveitando que $b_{ij} \equiv a_i \mod p$ e tomando os elementos de $\{b_{ij}\}_{1 \le i < p_n}$ módulo *p*, tem-se que existe um SRR $\mod p$ contido em $\{a_i\}_{1 \le i < p_n}$. Portanto a condição (ii) também é satisfeita e o teorema 2 está demonstrado.

Note que conforme o Teorema Chinês do Resto o sistema [*] tem, para cada *i*, uma única solução módulo $p_1 p_2 \cdots p_n$ na incógnita a_i. O método de resolução desse sistema pode ser encontrado em livros de Teoria dos Números.

Um exemplo

A matriz

$$\left(b_{ij}\right)=\begin{bmatrix} 1 & 1 & 1 \\ 1 & 2 & 2 \\ -1 & -2 & -2 \\ -1 & -1 & -1 \end{bmatrix}$$

satisfaz as condições do teorema 2. Resolvendo os supracitados sistemas [*] correspondentes, tem-se $a_1=1, a_2=17, a_3=-17, a_4=-1$ donde o polinômio procurado é

$$P(x)=(x-1)(x-17)(x+17)(x+1)=\left(x^2-1\right)\left(x^2-289\right)\equiv$$
$$\equiv\left(x^2-1\right)\left(x^2-19\right)\equiv x^4+10x^2+19 \mod 30$$

Assim, se $5<x<7^2$ então x é primo se e só se $5^{\#}=30$ divide $x^4+10x^2+19\equiv P(x) \mod 30$

Conclusão

Os números primos suscitam várias questões interessantes. Ao contrário do que alguns matemáticos pensam, existe uma fértil diversidade de fórmulas que produzem ou caracterizam primos.

12

Produzindo Números Primos por Iteração

Introdução

Conforme o Dicionário Aurélio, *Iteração* é o "Processo de resolução (de uma equação, de um problema) mediante uma seqüência finita de operações em que o objeto de cada uma é o resultado da que a precede". O objetivo desta nota é apresentar fórmulas iteradas, ou de caráter iterado, que produzem todos os números primos, e somente primos.

Certamente $\pi(n)$ é uma das mais importantes funções da Teoria dos Números. O valor de $\pi(n)$ é, simplesmente, a quantidade de números primos no intervalo $[1,n]$. É possível escrever fórmulas elementares para $\pi(n)$. Mostraremos um meio elegante de fazer isto.

Um aviso

Apesar da existência de fórmulas elementares para $\pi(n)$, os algoritmos conhecidos, incluindo o que será apresentado, são bastante *lentos* para calcular o valor dessa função. Entende-se por *lento* um algoritmo que calcula o valor de $f(n)$ num tempo que, para n suficientemente grande, é maior que qualquer potência de $\log n$. Note que $\log n$ é, proporcionalmente, uma aproximação do número de algarismos de n. Por isso o logaritmo surge de modo natural: um cálculo tende a ser tanto mais trabalhoso quantos forem os algarismos dos números envolvidos.

Fórmulas

Em Teoria dos Números é comum representar por $n^\#$ o produto dos primos que não excedem *n*. Assim, $2^\# = 2;\ 3^\# = 4^\# = 6;\ 5^\# = 6^\# = 30;$ etc. O número $n^\#$ chama-se o *primorial de n*, numa alusão ao fatorial.

A idéia central é que há uma sucessão (a_n) de inteiros, definida iteradamente, de modo elementar e intuitivo, satisfazendo $a_1 = a_2 = 1$ e $a_{n+1} = n^\#$, para $n > 1$. Basta definir a sucessão (a_n) por

$$\begin{cases} a_1 = 1 \\ a_{n+1} = a_n n^{\lfloor 1/\mathrm{mdc}(a_n,n)\rfloor}, \text{ para } n \geq 1 \end{cases}$$ onde $\lfloor x \rfloor$ representa o maior inteiro que não excede *x*.

É fácil ver que $a_2 = 1$ e que para *n*=2, $a_{n+1} = n^\#$. Mostrarei que esta igualdade também vale para *n*>2. Suponha, por indução, que $a_n = (n-1)^\#$ para algum inteiro $n > 2$. Se *n* é primo, $\mathrm{mdc}(a_n, n) = 1$, donde $\lfloor 1/\mathrm{mdc}(a_n, n)\rfloor = 1$ e portanto $a_{n+1} = a_n n^1 = (n-1)^\# n = n^\#$. Se *n* não é primo, então $\mathrm{mdc}(a_n, n) > 1$ donde $\lfloor 1/\mathrm{mdc}(a_n, n)\rfloor = 0$, e portanto $a_{n+1} = a_n n^0 = a_n = (n-1)^\# = n^\#$. Em qualquer caso tem-se $a_{n+1} = n^\#$, sempre que $a_n = (n-1)^\#$. Assim, fica provado por indução que $a_{n+1} = n^\#$, para todo inteiro *n*>1. Logo, as seguintes funções *f*, *g* produzem todos os números primos, e somente primos:

$$f(n) = \max\left(2, \frac{a_{n+1}}{a_n}\right), \text{ de modo que } f(n) = \begin{cases} n, \text{ se } n \text{ é primo} \\ 2, \text{ caso contrário} \end{cases}$$

$$\begin{cases} g(1) = 2 \\ g(n) = \max\left(g(n-1), a_{n+1}/a_n\right), \text{ para } n > 1 \end{cases}$$

sendo $g(n) = \begin{cases} \text{menor primo maior ou igual a } n, \text{ se } n \leq 2 \\ \text{maior primo menor ou igual a } n, \text{ se } n > 2 \end{cases}.$

Além disso, tem-se

$$\frac{a_i}{a_{i+1}} = \begin{cases} 1/i, \text{ se } i \text{ é primo} \\ 1, \text{ caso contrário} \end{cases}, \text{ logo } \left\lfloor \frac{a_i}{a_{i+1}} \right\rfloor = \begin{cases} 0 \quad \text{se } i \text{ é primo} \\ 1 \quad \text{caso contrário} \end{cases}, \text{ daí } \pi(n) = n - \sum_{i=1}^{n} \left\lfloor \frac{a_i}{a_{i+1}} \right\rfloor .$$

Não é razoável calcular números primos nem os valores de $\pi(n)$ usando as fórmulas apresentadas. Há meios mais rápidos de fazer isto. Entretanto, este fato não as desmerece, pois elas têm interesse teórico. São apreciadas pelas relações matemáticas que evidenciam e por sua elegância.

13

Uma Constante para os Números Primos

Um meio de construir fórmulas para primos é escrevê-los de modo codificado sob a forma de números reais. Estes números, muitas vezes, são definidos como limites de sucessões ou como somas infinitas, construídas a partir dos números primos que codificam. Um exemplo disso, longe de ser o único, é o número real η = 0,01101010001010..., onde o n-ésimo dígito a direita da vírgula é 1 se n for primo, e é 0 caso contrário. Como os únicos dígitos de η são 0 e 1, é natural considerá-lo escrito na base 2, de modo que, sendo p_n o n-ésimo número primo, tem-se:

$$\eta = \sum_{n=1}^{\infty} \frac{1}{2^{p_n}}$$

Na base 10 escreve-se η = 0,414682509851111166...

Uma observação

Seja $\lfloor x \rfloor$ o único inteiro tal que $x - 1 < \lfloor x \rfloor \le x$. Considerando o modo como η é construído, não é difícil ver que:

$$(*) \qquad \lfloor 2^n \eta \rfloor - 2\lfloor 2^{n-1}\eta \rfloor = \begin{cases} 1 \text{ se } n \text{ é primo} \\ 0 \text{ caso contrário} \end{cases}$$

Isso porque a expressão acima produz o n-ésimo algarismo à direita da vírgula de η, quando escrito na base 2. É de fácil verificação que, de modo mais geral, dado um inteiro b>1, e um real positivo r, tem-se:

$$\lfloor b^n r \rfloor - b\lfloor b^{n-1} r \rfloor = r_n$$

onde r_n é o n-ésimo dígito à direita da vírgula de r quando o escrevemos na base b.

A função π

Os matemáticos denotam a quantidade de números primos menores ou iguais a x, por $\pi(x)$. A função π (que não deve ser confundida com a célebre constante 3,14159...) é conhecida em língua inglesa como *prime counting function*, e tem um papel importante em Teoria dos Números. Conforme a igualdade (∗), para todo inteiro positivo n, vale

$$\pi(n) = \sum_{i=1}^{n} \left(\lfloor 2^i \eta \rfloor - 2 \lfloor 2^{i-1} \eta \rfloor \right)$$

Expandindo a soma e simplificando ter-se-á

$$\pi(n) = 2\lfloor 2^n \eta \rfloor - \sum_{i=1}^{n} \lfloor 2^i \eta \rfloor$$

Servimo-nos, portanto, do real η para exprimir os valores da função π.

Uma função para os números primos

Ainda aproveitando a igualdade (∗), é fácil ver que a seguinte função f, definida para os inteiros positivos, produz todos os números primos, e apenas primos:

$$f(n) = 2 + (n-2)\left(\lfloor 2^n \eta \rfloor - 2\lfloor 2^{n-1} \eta \rfloor \right)$$

De fato, se n é primo, então $f(n) = n$, e portanto, $f(n)$ também é primo (logo f gera todos os primos). Por outro lado, se n não é primo, $f(n) = 2$. Em qualquer caso, $f(n)$ é primo.

Uma função para o *n*-ésimo número primo

Sebastian Martin Ruiz e Jonathan Sondow observaram que uma conseqüência imediata das desigualdades demonstradas por Rosser e Schoenfeld em 1962 é que

$$p_n \le 2 + 2n\log n < p_{2n}$$

portanto, como

$$1 - \left\lfloor \frac{\pi(i)}{n} \right\rfloor = \begin{cases} 1 & \text{se } i < p_n \\ 0 & \text{se } p_n \le i < p_{2n} \end{cases}$$

tem-se

$$p_n = 1 + \sum_{i=1}^{p_{2n}-1} \left(1 - \left\lfloor \frac{\pi(i)}{n} \right\rfloor\right) = 1 + \sum_{i=1}^{\lfloor 2+2n\log n \rfloor} \left(1 - \left\lfloor \frac{\pi(i)}{n} \right\rfloor\right)$$

$$p_n = 3 + \lfloor 2n\log n \rfloor - \sum_{i=1}^{\lfloor 2+2n\log n \rfloor} \left\lfloor \frac{\pi(i)}{n} \right\rfloor$$

Vimos que $\pi(n) = 2\lfloor 2^n \eta \rfloor - \sum_{i=1}^{n} \lfloor 2^i \eta \rfloor$, então, por simples substituição

$$p_n = 3 + \lfloor 2n\log n \rfloor - \sum_{i=1}^{\lfloor 2+2n\log n \rfloor} \left\lfloor \frac{1}{n}\left(2\lfloor 2^i \eta \rfloor - \sum_{j=1}^{i} \lfloor 2^j \eta \rfloor\right) \right\rfloor$$

Outros reais que codificam primos

Uma questão é saber se existe alguma seqüência crescente (q_n) de números primos tal que $\eta_q = \sum_{i=1}^{\infty} \frac{1}{2^{q_i}}$ seja algébrico.

Em caso positivo haveria um modo rápido de produzir primos arbitrariamente grandes, desde que se conhecesse o número algébrico η_q. É uma possibilidade razoável já que existem "muitas" escolhas possíveis para η_q. De fato, para cada sucessão crescente (q_n) de números primos, existe um real η_q distinto, e como existe uma quantidade não enumerável de tais sucessões, há também uma infinidade não enumerável de reais η_q.

Note que é trivial mostrar que cada η_q é irracional. Basta observar que sua representação binária não é periódica.

14

Primalidade e Número de Divisores

Introdução

Seja n um inteiro positivo e $\mathrm{d}(n)$ o número de inteiros positivos que o dividem. É claro que n é primo se e só se $\mathrm{d}(n) = 2$. Existe, entretanto, um modo menos trivial de estabelecermos a primalidade de n usando $\mathrm{d}(n)$. Um inteiro p é primo se, e somente se, pudermos escrevê-lo como $p = n^{1/(d(n)-1)}$, para algum inteiro n. Isto é, todo número natural da forma $n^{1/(d(n)-1)}$ é primo, e todo número primo pode ser escrito deste modo. O objetivo desta nota é provar isso e apresentar uma fórmula para números primos amparada nessa proposição. Também será apresentada uma fórmula para a função Λ de Von Mangoldt, que é definida por $\Lambda(n) = \log p$ se n é potência do primo p e $\Lambda(n) = 0$ nos outros casos. Seguem-se as

Fórmulas

(i) $\Lambda(n) = \log \max\left(\mathbb{Z} \cap \left\{1, n^{1/(d(n)-1)}\right\}\right)$

(ii) $f(n) = \max\left(\mathbb{Z} \cap \left\{2, n^{1/(d(n)-1)}\right\}\right) =$ número primo

O leitor deve notar que ambas fundamentam-se na seguinte

Proposição. Seja $n \in \mathbb{Z}$, $n>1$. Se $g(n) = n^{1/(\mathrm{d}(n)-1)} \in \mathbb{Z}$ então $g(n)$ é um número primo.

Prova. Suponha que *n* é potência de um número primo *p*, digamos, $n = p^k$. Então $\mathrm{d}(n) = k+1$ e $g(n) = n^{1/(\mathrm{d}(n)-1)} = \left(p^k\right)^{1/((k+1)-1)} = \left(p^k\right)^{1/k} = p$, donde $g(n) = p$ é primo. Portanto, se *n* é potência de um número primo *p* então $g(n) = p$ é primo e neste caso a proposição é verdadeira.

Mostraremos agora que se *n* não é potência de primo, então $g(n)$ não é inteiro. Isto é o mesmo que mostrar que se $g(n)$ é inteiro, então *n* é potência de primo. Assim, ter-se-á $g(n) \in \mathbb{Z} \Rightarrow n \text{ é potência de primo} \Rightarrow g(n) \text{ é primo}$, e a proposição estará provada.

Suponha por absurdo que exista $n \in \mathbb{Z}$, $n>1$ tal que $g(n)$ é inteiro e *n* não é potência de primo. Então existem primos distintos *p*, *q* tais que $q|n$ e $p|n$ e portanto $p|g(n)$. Seja p^k a maior potência de *p* que divide *n*. Como d é função multiplicativa, isto é, $\mathrm{d}(uv)=\mathrm{d}(u)\mathrm{d}(v)$ sempre que *u* e *v* forem relativamente primos, então

$$\mathrm{d}(n) \geq \mathrm{d}\left(p^k\right)\mathrm{d}(q) = (k+1)(2) = 2k+2 \Rightarrow \mathrm{d}(n) \geq 2k+2 \Rightarrow$$
$$\Rightarrow \mathrm{d}(n) - 1 > 2k \Rightarrow g(n)^{2k} \mid g(n)^{d(n)-1} \Rightarrow g(n)^{2k} \mid n$$

Como $p \mid g(n)$ e $g(n)^{2k} \mid n$ então $p^{2k} \mid n$. Eis o absurdo, pois por hipótese p^k é a *maior* potência de *p* que divide *n*. Fica, assim, provada a proposição e as fórmulas (i) e (ii) seguem-se trivialmente.

15

Outras Fórmulas e Conjecturas

Não poderia deixar de incluir aqui as duas últimas fórmulas nas quais tenho trabalhado. Com uma ponta de pesar, confesso não tê-las, ainda, lustrado com o devido rigor da demonstração, como convém aos bons trabalhos em Matemática. Não obstante, acredito não estar longe da verdade pois os testes que empreendi com software de computação algébrica (Maple) só fizeram reforçar minha crença. Além disso, se as proposições abaixo enunciadas não são verdadeiras, são pelo menos muitos elegantes e indicam alternativas de pesquisa neste ramo da Matemática.

Uma fórmula otimista

Conjectura 1. Existe um número real $c > 0$ tal que $f(n) = \lfloor cn!^2 \rfloor$ é primo para todo inteiro positivo *n*, onde $n!^2$ é o quadrado do fatorial de *n* e $\lfloor x \rfloor$ é o maior inteiro menor ou igual a *x*.

Conjectura 2. O menor valor para *c* que torna a conjectura 1 verdadeira, com 600 algarismos a direita da vírgula, é dado por

$$
\begin{aligned}
c = 2,\ & 81132161152377067131230743440082128426483186556243159712765 2\\
& 046416586423901874748464636222288303235789636697829126440086\\
& 848189987904285365047365511634550507895672134720433189832279\\
& 689750341055421752958090071609528340588245795276296334013701\\
& 648925202734400332662922789939943496564366989682290158979946\\
& 718294005449788129649056197463450850352723871460613578585385\\
& 986235704571979829149774929603747524163815289710467466667265\\
& 998128649483150791182219091215560675438465310257069900405819\\
& 866847487633698061095801325578681442858027459630222036432419\\
& 164796718341024210817985139058200061754042971659377005529956
\end{aligned}
$$

Para este valor de c, os primeiros 20 números primos produzidos pela fórmula $f(n)=\lfloor cn!^2 \rfloor$ da conjectura 1 são:

n	$f(n)=\lfloor cn!^2 \rfloor$	n	$f(n)=\lfloor cn!^2 \rfloor$
1	2	11	4479421882434643
2	11	12	645036751070588593
3	101	13	109011210930929472311
4	1619	14	21366197342462176573007
5	40483	15	4807394402053989728926577
6	1457389	16	1230692966925821370605203741
7	71412067	17	355670267441562376104903881179
8	4570372291	18	115237166651066209857988857502039
9	370200155573	19	41600617161034901758733977558236253
10	37020015557311	20	16640246864413960703493591023294501227

Com o valor de c dado pela conjectura 2 pode-se calcular com precisão os primeiros 165 números primos $f(1), f(2), f(3), \ldots, f(165)$ da fórmula supracitada, sendo que $f(165)$ tem 592 algarismos.

Chamo a fórmula $f(n)=\lfloor cn!^2 \rfloor$ de *otimista* porque precisamos ser realmente bastante otimistas para supor que ela produza infinitos primos. De fato, a demonstração desta fórmula está condicionada a existência de números primos em intervalos bastante estreitos.

Uma fórmula fatorial

É fácil mostrar que se j, k, n, p são inteiros positivos satisfazendo $p=\sqrt[j]{kn!+1}<(n+1)^2$ então p é necessariamente um número primo. Por outro lado, uma tarefa menos trivial é provar a seguinte

Conjectura 3. Todo número primo $p < (n+1)^2$ pode ser escrito como $p = \sqrt[j]{kn!+1}$ para certos *j*, *k*, *n* inteiros positivos.

Alguns exemplos que satisfazem a conjectura 3 são os seguintes:

$\sqrt[1]{1\times 1!+1} = 2 < 2^2$ $\sqrt{1\times 5!+1} = 11 < 6^2$ $\sqrt{7\times 5!+1} = 29 < 6^2$

$\sqrt{8\times 5!+1} = 31 < 6^2$ $\sqrt[4]{2603\times 6!+1} = 37 < 7^2$ $\sqrt[6]{6597367\times 6!+1} = 41 < 7^2$

Munido de uma calculadora de bolso é bastante fácil escrever todos os primos $p < 40$ no formato $p = \sqrt[j]{kn!+1} < (n+1)^2$, conforme a conjectura 3. Também é fácil construir uma fórmula para primos utilizando a conjectura 3, caso ela seja verdadeira.

Tábua de Números Primos

n	p_n	n	p_n	n	p_n	n	p_n	n	p_n	n	p_n
1	**2**	41	**179**	81	**419**	121	**661**	161	**947**	201	**1229**
2	**3**	42	**181**	82	**421**	122	**673**	162	**953**	202	**1231**
3	**5**	43	**191**	83	**431**	123	**677**	163	**967**	203	**1237**
4	**7**	44	**193**	84	**433**	124	**683**	164	**971**	204	**1249**
5	**11**	45	**197**	85	**439**	125	**691**	165	**977**	205	**1259**
6	**13**	46	**199**	86	**443**	126	**701**	166	**983**	206	**1277**
7	**17**	47	**211**	87	**449**	127	**709**	167	**991**	207	**1279**
8	**19**	48	**223**	88	**457**	128	**719**	168	**997**	208	**1283**
9	**23**	49	**227**	89	**461**	129	**727**	169	**1009**	209	**1289**
10	**29**	50	**229**	90	**463**	130	**733**	170	**1013**	210	**1291**
11	**31**	51	**233**	91	**467**	131	**739**	171	**1019**	211	**1297**
12	**37**	52	**239**	92	**479**	132	**743**	172	**1021**	212	**1301**
13	**41**	53	**241**	93	**487**	133	**751**	173	**1031**	213	**1303**
14	**43**	54	**251**	94	**491**	134	**757**	174	**1033**	214	**1307**
15	**47**	55	**257**	95	**499**	135	**761**	175	**1039**	215	**1319**
16	**53**	56	**263**	96	**503**	136	**769**	176	**1049**	216	**1321**
17	**59**	57	**269**	97	**509**	137	**773**	177	**1051**	217	**1327**
18	**61**	58	**271**	98	**521**	138	**787**	178	**1061**	218	**1361**
19	**67**	59	**277**	99	**523**	139	**797**	179	**1063**	219	**1367**
20	**71**	60	**281**	100	**541**	140	**809**	180	**1069**	220	**1373**
21	**73**	61	**283**	101	**547**	141	**811**	181	**1087**	221	**1381**
22	**79**	62	**293**	102	**557**	142	**821**	182	**1091**	222	**1399**
23	**83**	63	**307**	103	**563**	143	**823**	183	**1093**	223	**1409**
24	**89**	64	**311**	104	**569**	144	**827**	184	**1097**	224	**1423**
25	**97**	65	**313**	105	**571**	145	**829**	185	**1103**	225	**1427**
26	**101**	66	**317**	106	**577**	146	**839**	186	**1109**	226	**1429**
27	**103**	67	**331**	107	**587**	147	**853**	187	**1117**	227	**1433**
28	**107**	68	**337**	108	**593**	148	**857**	188	**1123**	228	**1439**
29	**109**	69	**347**	109	**599**	149	**859**	189	**1129**	229	**1447**
30	**113**	70	**349**	110	**601**	150	**863**	190	**1151**	230	**1451**
31	**127**	71	**353**	111	**607**	151	**877**	191	**1153**	231	**1453**
32	**131**	72	**359**	112	**613**	152	**881**	192	**1163**	232	**1459**
33	**137**	73	**367**	113	**617**	153	**883**	193	**1171**	233	**1471**
34	**139**	74	**373**	114	**619**	154	**887**	194	**1181**	234	**1481**
35	**149**	75	**379**	115	**631**	155	**907**	195	**1187**	235	**1483**
36	**151**	76	**383**	116	**641**	156	**911**	196	**1193**	236	**1487**
37	**157**	77	**389**	117	**643**	157	**919**	197	**1201**	237	**1489**
38	**163**	78	**397**	118	**647**	158	**929**	198	**1213**	238	**1493**
39	**167**	79	**401**	119	**653**	159	**937**	199	**1217**	239	**1499**
40	**173**	80	**409**	120	**659**	160	**941**	200	**1223**	240	**1511**

n	p_n	n	p_n	n	p_n	n	p_n	n	p_n	n	p_n
241	**1523**	281	**1823**	321	**2131**	361	**2437**	401	**2749**	441	**3083**
242	**1531**	282	**1831**	322	**2137**	362	**2441**	402	**2753**	442	**3089**
243	**1543**	283	**1847**	323	**2141**	363	**2447**	403	**2767**	443	**3109**
244	**1549**	284	**1861**	324	**2143**	364	**2459**	404	**2777**	444	**3119**
245	**1553**	285	**1867**	325	**2153**	365	**2467**	405	**2789**	445	**3121**
246	**1559**	286	**1871**	326	**2161**	366	**2473**	406	**2791**	446	**3137**
247	**1567**	287	**1873**	327	**2179**	367	**2477**	407	**2797**	447	**3163**
248	**1571**	288	**1877**	328	**2203**	368	**2503**	408	**2801**	448	**3167**
249	**1579**	289	**1879**	329	**2207**	369	**2521**	409	**2803**	449	**3169**
250	**1583**	290	**1889**	330	**2213**	370	**2531**	410	**2819**	450	**3181**
251	**1597**	291	**1901**	331	**2221**	371	**2539**	411	**2833**	451	**3187**
252	**1601**	292	**1907**	332	**2237**	372	**2543**	412	**2837**	452	**3191**
253	**1607**	293	**1913**	333	**2239**	373	**2549**	413	**2843**	453	**3203**
254	**1609**	294	**1931**	334	**2243**	374	**2551**	414	**2851**	454	**3209**
255	**1613**	295	**1933**	335	**2251**	375	**2557**	415	**2857**	455	**3217**
256	**1619**	296	**1949**	336	**2267**	376	**2579**	416	**2861**	456	**3221**
257	**1621**	297	**1951**	337	**2269**	377	**2591**	417	**2879**	457	**3229**
258	**1627**	298	**1973**	338	**2273**	378	**2593**	418	**2887**	458	**3251**
259	**1637**	299	**1979**	339	**2281**	379	**2609**	419	**2897**	459	**3253**
260	**1657**	300	**1987**	340	**2287**	380	**2617**	420	**2903**	460	**3257**
261	**1663**	301	**1993**	341	**2293**	381	**2621**	421	**2909**	461	**3259**
262	**1667**	302	**1997**	342	**2297**	382	**2633**	422	**2917**	462	**3271**
263	**1669**	303	**1999**	343	**2309**	383	**2647**	423	**2927**	463	**3299**
264	**1693**	304	**2003**	344	**2311**	384	**2657**	424	**2939**	464	**3301**
265	**1697**	305	**2011**	345	**2333**	385	**2659**	425	**2953**	465	**3307**
266	**1699**	306	**2017**	346	**2339**	386	**2663**	426	**2957**	466	**3313**
267	**1709**	307	**2027**	347	**2341**	387	**2671**	427	**2963**	467	**3319**
268	**1721**	308	**2029**	348	**2347**	388	**2677**	428	**2969**	468	**3323**
269	**1723**	309	**2039**	349	**2351**	389	**2683**	429	**2971**	469	**3329**
270	**1733**	310	**2053**	350	**2357**	390	**2687**	430	**2999**	470	**3331**
271	**1741**	311	**2063**	351	**2371**	391	**2689**	431	**3001**	471	**3343**
272	**1747**	312	**2069**	352	**2377**	392	**2693**	432	**3011**	472	**3347**
273	**1753**	313	**2081**	353	**2381**	393	**2699**	433	**3019**	473	**3359**
274	**1759**	314	**2083**	354	**2383**	394	**2707**	434	**3023**	474	**3361**
275	**1777**	315	**2087**	355	**2389**	395	**2711**	435	**3037**	475	**3371**
276	**1783**	316	**2089**	356	**2393**	396	**2713**	436	**3041**	476	**3373**
277	**1787**	317	**2099**	357	**2399**	397	**2719**	437	**3049**	477	**3389**
278	**1789**	318	**2111**	358	**2411**	398	**2729**	438	**3061**	478	**3391**
279	**1801**	319	**2113**	359	**2417**	399	**2731**	439	**3067**	479	**3407**
280	**1811**	320	**2129**	360	**2423**	400	**2741**	440	**3079**	480	**3413**

n	p_n	n	p_n	n	p_n	n	p_n	n	p_n	n	p_n
481	**3433**	521	**3733**	561	**4073**	601	**4421**	641	**4759**	681	**5099**
482	**3449**	522	**3739**	562	**4079**	602	**4423**	642	**4783**	682	**5101**
483	**3457**	523	**3761**	563	**4091**	603	**4441**	643	**4787**	683	**5107**
484	**3461**	524	**3767**	564	**4093**	604	**4447**	644	**4789**	684	**5113**
485	**3463**	525	**3769**	565	**4099**	605	**4451**	645	**4793**	685	**5119**
486	**3467**	526	**3779**	566	**4111**	606	**4457**	646	**4799**	686	**5147**
487	**3469**	527	**3793**	567	**4127**	607	**4463**	647	**4801**	687	**5153**
488	**3491**	528	**3797**	568	**4129**	608	**4481**	648	**4813**	688	**5167**
489	**3499**	529	**3803**	569	**4133**	609	**4483**	649	**4817**	689	**5171**
490	**3511**	530	**3821**	570	**4139**	610	**4493**	650	**4831**	690	**5179**
491	**3517**	531	**3823**	571	**4153**	611	**4507**	651	**4861**	691	**5189**
492	**3527**	532	**3833**	572	**4157**	612	**4513**	652	**4871**	692	**5197**
493	**3529**	533	**3847**	573	**4159**	613	**4517**	653	**4877**	693	**5209**
494	**3533**	534	**3851**	574	**4177**	614	**4519**	654	**4889**	694	**5227**
495	**3539**	535	**3853**	575	**4201**	615	**4523**	655	**4903**	695	**5231**
496	**3541**	536	**3863**	576	**4211**	616	**4547**	656	**4909**	696	**5233**
497	**3547**	537	**3877**	577	**4217**	617	**4549**	657	**4919**	697	**5237**
498	**3557**	538	**3881**	578	**4219**	618	**4561**	658	**4931**	698	**5261**
499	**3559**	539	**3889**	579	**4229**	619	**4567**	659	**4933**	699	**5273**
500	**3571**	540	**3907**	580	**4231**	620	**4583**	660	**4937**	700	**5279**
501	**3581**	541	**3911**	581	**4241**	621	**4591**	661	**4943**	701	**5281**
502	**3583**	542	**3917**	582	**4243**	622	**4597**	662	**4951**	702	**5297**
503	**3593**	543	**3919**	583	**4253**	623	**4603**	663	**4957**	703	**5303**
504	**3607**	544	**3923**	584	**4259**	624	**4621**	664	**4967**	704	**5309**
505	**3613**	545	**3929**	585	**4261**	625	**4637**	665	**4969**	705	**5323**
506	**3617**	546	**3931**	586	**4271**	626	**4639**	666	**4973**	706	**5333**
507	**3623**	547	**3943**	587	**4273**	627	**4643**	667	**4987**	707	**5347**
508	**3631**	548	**3947**	588	**4283**	628	**4649**	668	**4993**	708	**5351**
509	**3637**	549	**3967**	589	**4289**	629	**4651**	669	**4999**	709	**5381**
510	**3643**	550	**3989**	590	**4297**	630	**4657**	670	**5003**	710	**5387**
511	**3659**	551	**4001**	591	**4327**	631	**4663**	671	**5009**	711	**5393**
512	**3671**	552	**4003**	592	**4337**	632	**4673**	672	**5011**	712	**5399**
513	**3673**	553	**4007**	593	**4339**	633	**4679**	673	**5021**	713	**5407**
514	**3677**	554	**4013**	594	**4349**	634	**4691**	674	**5023**	714	**5413**
515	**3691**	555	**4019**	595	**4357**	635	**4703**	675	**5039**	715	**5417**
516	**3697**	556	**4021**	596	**4363**	636	**4721**	676	**5051**	716	**5419**
517	**3701**	557	**4027**	597	**4373**	637	**4723**	677	**5059**	717	**5431**
518	**3709**	558	**4049**	598	**4391**	638	**4729**	678	**5077**	718	**5437**
519	**3719**	559	**4051**	599	**4397**	639	**4733**	679	**5081**	719	**5441**
520	**3727**	560	**4057**	600	**4409**	640	**4751**	680	**5087**	720	**5443**

n	p_n	n	p_n	n	p_n	n	p_n	n	p_n	n	p_n
721	**5449**	761	**5801**	801	**6143**	841	**6481**	881	**6841**	921	**7211**
722	**5471**	762	**5807**	802	**6151**	842	**6491**	882	**6857**	922	**7213**
723	**5477**	763	**5813**	803	**6163**	843	**6521**	883	**6863**	923	**7219**
724	**5479**	764	**5821**	804	**6173**	844	**6529**	884	**6869**	924	**7229**
725	**5483**	765	**5827**	805	**6197**	845	**6547**	885	**6871**	925	**7237**
726	**5501**	766	**5839**	806	**6199**	846	**6551**	886	**6883**	926	**7243**
727	**5503**	767	**5843**	807	**6203**	847	**6553**	887	**6899**	927	**7247**
728	**5507**	768	**5849**	808	**6211**	848	**6563**	888	**6907**	928	**7253**
729	**5519**	769	**5851**	809	**6217**	849	**6569**	889	**6911**	929	**7283**
730	**5521**	770	**5857**	810	**6221**	850	**6571**	890	**6917**	930	**7297**
731	**5527**	771	**5861**	811	**6229**	851	**6577**	891	**6947**	931	**7307**
732	**5531**	772	**5867**	812	**6247**	852	**6581**	892	**6949**	932	**7309**
733	**5557**	773	**5869**	813	**6257**	853	**6599**	893	**6959**	933	**7321**
734	**5563**	774	**5879**	814	**6263**	854	**6607**	894	**6961**	934	**7331**
735	**5569**	775	**5881**	815	**6269**	855	**6619**	895	**6967**	935	**7333**
736	**5573**	776	**5897**	816	**6271**	856	**6637**	896	**6971**	936	**7349**
737	**5581**	777	**5903**	817	**6277**	857	**6653**	897	**6977**	937	**7351**
738	**5591**	778	**5923**	818	**6287**	858	**6659**	898	**6983**	938	**7369**
739	**5623**	779	**5927**	819	**6299**	859	**6661**	899	**6991**	939	**7393**
740	**5639**	780	**5939**	820	**6301**	860	**6673**	900	**6997**	940	**7411**
741	**5641**	781	**5953**	821	**6311**	861	**6679**	901	**7001**	941	**7417**
742	**5647**	782	**5981**	822	**6317**	862	**6689**	902	**7013**	942	**7433**
743	**5651**	783	**5987**	823	**6323**	863	**6691**	903	**7019**	943	**7451**
744	**5653**	784	**6007**	824	**6329**	864	**6701**	904	**7027**	944	**7457**
745	**5657**	785	**6011**	825	**6337**	865	**6703**	905	**7039**	945	**7459**
746	**5659**	786	**6029**	826	**6343**	866	**6709**	906	**7043**	946	**7477**
747	**5669**	787	**6037**	827	**6353**	867	**6719**	907	**7057**	947	**7481**
748	**5683**	788	**6043**	828	**6359**	868	**6733**	908	**7069**	948	**7487**
749	**5689**	789	**6047**	829	**6361**	869	**6737**	909	**7079**	949	**7489**
750	**5693**	790	**6053**	830	**6367**	870	**6761**	910	**7103**	950	**7499**
751	**5701**	791	**6067**	831	**6373**	871	**6763**	911	**7109**	951	**7507**
752	**5711**	792	**6073**	832	**6379**	872	**6779**	912	**7121**	952	**7517**
753	**5717**	793	**6079**	833	**6389**	873	**6781**	913	**7127**	953	**7523**
754	**5737**	794	**6089**	834	**6397**	874	**6791**	914	**7129**	954	**7529**
755	**5741**	795	**6091**	835	**6421**	875	**6793**	915	**7151**	955	**7537**
756	**5743**	796	**6101**	836	**6427**	876	**6803**	916	**7159**	956	**7541**
757	**5749**	797	**6113**	837	**6449**	877	**6823**	917	**7177**	957	**7547**
758	**5779**	798	**6121**	838	**6451**	878	**6827**	918	**7187**	958	**7549**
759	**5783**	799	**6131**	839	**6469**	879	**6829**	919	**7193**	959	**7559**
760	**5791**	800	**6133**	840	**6473**	880	**6833**	920	**7207**	960	**7561**

n	p_n	n	p_n	n	p_n	n	p_n	n	p_n	n	p_n
961	**7573**	1001	**7927**	1041	**8293**	1081	**8681**	1121	**9013**	1161	**9391**
962	**7577**	1002	**7933**	1042	**8297**	1082	**8689**	1122	**9029**	1162	**9397**
963	**7583**	1003	**7937**	1043	**8311**	1083	**8693**	1123	**9041**	1163	**9403**
964	**7589**	1004	**7949**	1044	**8317**	1084	**8699**	1124	**9043**	1164	**9413**
965	**7591**	1005	**7951**	1045	**8329**	1085	**8707**	1125	**9049**	1165	**9419**
966	**7603**	1006	**7963**	1046	**8353**	1086	**8713**	1126	**9059**	1166	**9421**
967	**7607**	1007	**7993**	1047	**8363**	1087	**8719**	1127	**9067**	1167	**9431**
968	**7621**	1008	**8009**	1048	**8369**	1088	**8731**	1128	**9091**	1168	**9433**
969	**7639**	1009	**8011**	1049	**8377**	1089	**8737**	1129	**9103**	1169	**9437**
970	**7643**	1010	**8017**	1050	**8387**	1090	**8741**	1130	**9109**	1170	**9439**
971	**7649**	1011	**8039**	1051	**8389**	1091	**8747**	1131	**9127**	1171	**9461**
972	**7669**	1012	**8053**	1052	**8419**	1092	**8753**	1132	**9133**	1172	**9463**
973	**7673**	1013	**8059**	1053	**8423**	1093	**8761**	1133	**9137**	1173	**9467**
974	**7681**	1014	**8069**	1054	**8429**	1094	**8779**	1134	**9151**	1174	**9473**
975	**7687**	1015	**8081**	1055	**8431**	1095	**8783**	1135	**9157**	1175	**9479**
976	**7691**	1016	**8087**	1056	**8443**	1096	**8803**	1136	**9161**	1176	**9491**
977	**7699**	1017	**8089**	1057	**8447**	1097	**8807**	1137	**9173**	1177	**9497**
978	**7703**	1018	**8093**	1058	**8461**	1098	**8819**	1138	**9181**	1178	**9511**
979	**7717**	1019	**8101**	1059	**8467**	1099	**8821**	1139	**9187**	1179	**9521**
980	**7723**	1020	**8111**	1060	**8501**	1100	**8831**	1140	**9199**	1180	**9533**
981	**7727**	1021	**8117**	1061	**8513**	1101	**8837**	1141	**9203**	1181	**9539**
982	**7741**	1022	**8123**	1062	**8521**	1102	**8839**	1142	**9209**	1182	**9547**
983	**7753**	1023	**8147**	1063	**8527**	1103	**8849**	1143	**9221**	1183	**9551**
984	**7757**	1024	**8161**	1064	**8537**	1104	**8861**	1144	**9227**	1184	**9587**
985	**7759**	1025	**8167**	1065	**8539**	1105	**8863**	1145	**9239**	1185	**9601**
986	**7789**	1026	**8171**	1066	**8543**	1106	**8867**	1146	**9241**	1186	**9613**
987	**7793**	1027	**8179**	1067	**8563**	1107	**8887**	1147	**9257**	1187	**9619**
988	**7817**	1028	**8191**	1068	**8573**	1108	**8893**	1148	**9277**	1188	**9623**
989	**7823**	1029	**8209**	1069	**8581**	1109	**8923**	1149	**9281**	1189	**9629**
990	**7829**	1030	**8219**	1070	**8597**	1110	**8929**	1150	**9283**	1190	**9631**
991	**7841**	1031	**8221**	1071	**8599**	1111	**8933**	1151	**9293**	1191	**9643**
992	**7853**	1032	**8231**	1072	**8609**	1112	**8941**	1152	**9311**	1192	**9649**
993	**7867**	1033	**8233**	1073	**8623**	1113	**8951**	1153	**9319**	1193	**9661**
994	**7873**	1034	**8237**	1074	**8627**	1114	**8963**	1154	**9323**	1194	**9677**
995	**7877**	1035	**8243**	1075	**8629**	1115	**8969**	1155	**9337**	1195	**9679**
996	**7879**	1036	**8263**	1076	**8641**	1116	**8971**	1156	**9341**	1196	**9689**
997	**7883**	1037	**8269**	1077	**8647**	1117	**8999**	1157	**9343**	1197	**9697**
998	**7901**	1038	**8273**	1078	**8663**	1118	**9001**	1158	**9349**	1198	**9719**
999	**7907**	1039	**8287**	1079	**8669**	1119	**9007**	1159	**9371**	1199	**9721**
1000	**7919**	1040	**8291**	1080	**8677**	1120	**9011**	1160	**9377**	1200	**9733**

Referências Bibliográficas

[1] RIBENBOIM, Paulo. Existem funções que geram os números primos?. *Revista Matemática Universitária*, Rio de Janeiro, n. 15, p. 1-12, dez. 1993.

[2] WATANABE, Renate. Uma fórmula para os números primos. *Revista do Professor de Matemática*, n. 37, p. 19-21, 1998.

[3] GUEDES, Eric. Uma construção de primos. *Revista do Professor de Matemática*, n. 15, p. 39-41, 1989.

[4] RIBENBOIM, Paulo. *The New Book of Prime Number Records.* 3. ed. Springer, 1996.

[5] COURANT, R, ROBBINS, H. *O que é Matemática?*: uma abordagem elementar de métodos e conceitos. Ciência Moderna.

[6] MEGA, Élio, WATANABE, Renate. *Olimpíadas Brasileiras de Matemática*: problemas e resoluções. Editora Núcleo, 1988. Problema 23.

[7] APOSTOL, T.M. *Introduction to Analytic Number Theory*. Springer-Verlag, New York, 1976.

[8] HARDY, G.W., WRITE, E.M. *An Introduction to the Theory of Numbers*. 5.ed. Oxford: Oxford University Press, 1979.

[9] LIMA, Elon Lages. *Curso de Análise, volume 1*. 8. ed. Rio de Janeiro, IMPA, CNPq, 1976. (Projeto Euclides).

[10] LIMA, Elon Lages. *Análise Real, volume 1.* Rio de Janeiro, IMPA, CNPq, 1989. (Coleção Matemática Universitária)

[11] FILHO, Edgard de Alencar. *Teoria das Congruências*. São Paulo: Nobel, 1986.

[12] GUIMARÃES, Ângelo de Moura, LAGES, Newton Alberto de Castilho. *Algoritmos e Estrutura de Dados*. Rio de Janeiro: LTC.

[13] RAMOS, Wilson C. da S. Polinômios gerando primos. *Revista do Professor de Matemática*, n.45, p.39-40, 2001.

[14] TENGAN, Eduardo. Séries formais. *Eureka!*, n.11, p.34-39, 2001.

[15] COUTINHO, S. C. *Primalidade em Tempo Polinomial*: Uma Introdução ao Algoritmo AKS. Rio de Janeiro: Sociedade Brasileira de Matemática, 2004. Coleção Iniciação Científica.